Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Троицкий Александр Витальевич

Подписано цифровой подписью: Троицкий Александр Витальевич

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.07 «ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.04.01 - Информационная безопасность
Направленность (профиль): Менеджмент информационной безопасности
Уровень высшего образования: магистратура
Форма обучения: очная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Воронов А.Н. Рабочая программа дисциплины (модуля): Теоретические основы компьютерной безопасности. – Королев МО: «Технологический Университет», 2023

Рецензент: Соляной В. Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки магистров 10.04.01 Информационная безопасность и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Соляной В.Н. к.в.н., доцент			
Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания кафедры	№8 от 29.03.2023г.			

Рабочая программа согласована:
Руководитель ОПОП ВО Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания УМС	Протокол № 5 от 11.04.2023г.			

2

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП

Целью изучения дисциплины является:

1. Сформировать у студентов базовые знания и практические навыки защиты информации в компьютерных системах.

2. Освоение студентами теоретических основ, технологий и механизмов защиты компьютерных систем.

В процессе обучения по направлению подготовки 10.04.01 «Информационная безопасность», студент приобретает и совершенствует следующие компетенции:

Универсальные компетенции:

- УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Профессиональные компетенции:

- ПК-3: Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности.

Основными **задачами** дисциплины являются:

1. Ознакомление студентов с теоретическими основами и нормативной базой, применяемых для построения защищенных информационных систем;
2. Формирование у студентов базовых знаний в области технологий и механизмов защиты информации, применяемых в компьютерных системах;
3. Привитие студентам навыков практической работы с программно-аппаратными средствами защиты информации;
4. Подготовка студентов применять стандарты по оценке информационной защищённости при анализе и проектировании защищённых компьютерных систем.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- УК-1.3 Использует методы системного и критического анализа, анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.
- ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.

Необходимые умения:

- УК-1.2. Определяет уязвимости и угрозы информационной безопасности, необходимые для выявления и решения проблемной ситуации, планирует мероприятия и процессы по их устранению на основе системного и междисциплинарных подходов.

- ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.

Необходимые знания:

- УК-1.1. Ставит цель, определяет способы ее достижения, разрабатывает стратегию действия, принимает конкретные решения для ее реализации с учетом требований регуляторов в области защиты информации.

- ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП ВО

Дисциплина «Теоретические основы компьютерной безопасности» Б1.В.07 относится к части, формируемой участниками образовательных отношений, блока 1 основной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: «Основы теории информационной безопасности», «Защищенные информационные системы» и компетенциях: ПК-1, 3; УК-1; ОПК-1.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при изучении дисциплин: “Информационная безопасность финансово-кредитных структур”, “Комплексная проверка информационной безопасности” и для написания магистерской диссертации.

3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для обучающихся очной формы составляет 3 зачетных единицы, 108 часов.

Таблица1

Виды занятий	**Всего часов**	**Семестр 2**	**Семестр …**	**Семестр …**	**Семестр …**
Общая трудоемкость	**108**	**108**			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**46**	**46**			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	8	8			
Другие виды контактной работы*	**6**	**6**			
Практическая подготовка	**нет**	**нет**			
Самостоятельная работа	**60**	**60**			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	-	-			
Вид итогового контроля	Экзамен	Экзамен			

* Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование.

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, час. Очное	Лабораторные работы, час. Очное	Занятия в интерактивной форме, час Очное	Код компетенций
	Третий семестр				
Раздел 1. Концептуально-теоретические основы компьютерной безопасности					
Тема 1. Введение. Основные понятия теории компьютерной безопасности	2	2	1	1	УК-1
Тема 2. Анализ угроз информационной безопасности для компьютерных систем	2	2	1	1	УК-1
Тема 3. Основные уровни защиты информации в компьютерных системах	2	2	1	1	УК-1
Тема 4. Основные положения формальной теории защиты информации	2	2	1	1	УК-1
Тема 5. Формальные модели безопасности	2	2	1	1	УК-1 ПК-3
Тема 6. Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам	2	2	1	1	УК-1 ПК-3
Тема 7. Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации	2	2	1	1	УК-1 ПК-3
Раздел 2. Прикладные основы теории компьютерной безопасности					

Наименование тем	Лекции, час. Очное	Практические занятия, час. Очное	Лабораторные работы, час. Очное	Занятия в интерактивной форме, час Очное	Код компетенций
Тема № 8. Методология обследования и проектирования защищенных информационных (автоматизированных) систем	1	1	1	1	УК-1 ПК-3
Тема № 9. Общие сведения о стандартах в области информационной безопасности. Стандарт «Критерии оценки доверенных компьютерных систем»/ TCSEC («Оранжевая книга»). Общие критерии оценки безопасности информационных технологий («Common Criteria»)	0,5	0.2	1	1	УК-1 ПК-3
Тема № 10. Концепция защиты СВТ и АС от НСД в соответствии с руководящими документами Гостехкомиссии и нормативно-методическими документами ФСТЭК России	0,5	0.5	2	2	УК-1 ПК-3
Итого:	16	16	8	8	

4.2. Содержание тем дисциплины

Раздел 1. Концептуально-теоретические основы компьютерной безопасности

Тема 1. Введение. Основные понятия теории компьютерной безопасности

Введение. Место и роль дисциплины в процессе подготовки магистра, связь с другими дисциплинами. Структура и содержание дисциплины. Виды занятий и контрольных мероприятий. Рекомендуемая литература.

Актуальность проблемы обеспечения информационной безопасности (ИБ) в компьютерных системах. Современная постановка целей и задач по обеспечению компьютерной безопасности (переход к тотальной защите и интенсивным мерам). Основные термины и определения в области ИБ компьютерных систем и сетей.

Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности. Факты, свидетельствующие о способах злоупотребления информацией, циркулирующей в компьютерных системах.

Тема 2. Анализ угроз информационной безопасности для компьютерных систем

Проблемы безопасности компьютерных систем (сетей). Понятие угрозы. Цели злоумышленников, осуществляющих основные атаки.

Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников. Уязвимости АС, возможные атаки на них. Особенности построения систем обнаружения атак (СОА) в АС. Фундаментальные угрозы – утечка информации, нарушение целостности, отказ в обслуживании, незаконное использование. Первичные угрозы – проникновение (маскарад, обход защиты, нарушение полномочий) и внедрение (троянские программы, потайные ходы).

Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.

Причины возникновения угроз безопасности информации. Отличительные особенности угроз корпоративным и локально-вычислительным сетям.

Тема 3. Основные уровни защиты информации в компьютерных системах

Организация системы безопасности по уровням компьютерных систем (КС). Уровни защиты, в соответствии с механизмами реагирования на угрозы. Способы защиты данных на различных уровнях. Организация системы безопасности по уровням.

Машинные носители информации (МНИ). Защита МНИ. Защита средств взаимодействия с МНИ.

Основные особенности компьютерной информации с точки зрения доступа к ней злоумышленников. Виды защищаемой компьютерной информации. Условия доступа к защищаемой информации со стороны злоумышленников.

Тема 4. Основные положения формальной теории защиты информации

Аксиомы и определения доступа субъектов к объектам. Понятие объекта относительно языка L. Объекты, входящие в состав КС. Язык описания клавиатуры. Преобразование. Пример преобразования. Инициирование действия преобразования. Два состояния преобразования. Понятие домена. Процесс. Определение субъекта. Виды доступа к субъекту. Информационный поток. Запись.

Аксиома доступа субъектов к объектам. Определение понятия разграничения доступа. Методы разграничения доступа.

Дискреционное разграничение доступа. Матрицы доступа. Списки полномочий.

Полномочное (мандатное) разграничение доступа. Разграничение по уровням секретности. Различие между дискреционным и мандатным разграничением доступа.

Тема № 5. Формальные модели безопасности

Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU). Моделирование поведения системы во времени. Основные команды и операции, моделирующие поведение системы. Примеры команд, используемых при переходе системы из одного состояния в другое. Формальное описание системы в модели HRU. Поведение системы во времени. Понятие монооперационной системы. Теорема о существовании алгоритма определения исходного состояния системы. Условие использования классической модели HRU. Разрешимость проблемы безопасности.

Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.

Граф доступов. Правила определения переходов системы из состояния в состояние. Условия реализации прав доступа. Расширенная модель Take-Grant, анализ информационных каналов.

Пути и стоимости возникновения информационных потоков в расширенной модели Take-Grant.

Тема № 6. Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам

Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.

Требования, предъявляемые к формированию политики безопасности организации. Структура и содержание политики безопасности организации применительно к компьютерным системам.

Тема № 7. Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации

Фрагментарный и комплексный подходы к созданию систем защиты. Основные достоинства и недостатки фрагментарного подхода. Организация защищенной среды обработки информации при комплексном подходе. Недостатки комплексного подхода. Условия эффективной работы средств защиты информации. Организация защиты субъектов информационных отношений.

Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации.

Построение систем защиты от угрозы нарушения конфиденциальности информации. Модель системы защиты от угроз нарушения конфиденциальности информации. Структура системы защиты от угроз нарушения конфиденциальности информации.

Построение систем защиты от угрозы нарушения целостности информации. Две основные группы организационно-технологических мер защиты целостности информации. Технологические меры контроля целостности битовых последовательностей, хранящихся на машинных носителях. Циклический контрольный код как механизм обеспечения контроля целостности информации. Интегрированный подход для обеспечения целостности данных. Основные принципы обеспечения целостности данных. Обеспечение защиты целостности программно-аппаратной среды.

Построение системы защиты от угрозы нарушения доступности информации. Понятие доступности информации. Основные угрозы доступности информации. Причины возникновения угроз доступности информации. Основные средства защиты от угрозы нарушения доступности информации.

Раздел 2. Прикладные основы теории компьютерной безопасности

Тема № 8. Методология обследования и проектирования защищенных информационных (автоматизированных) систем

Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи. Методы построения защищённых АС. Два основных метода проектирования. Метод проектирования «снизу вверх». Недостатки метода проектирования «снизу вверх». Иерархический метод построения защищённой АС («сверху вниз»). Принципы проектирования. Струк-

турный принцип и принцип модульного проектирования. Три основных конструкции для проектирования. Использование элемента DO-WHILE для организации цикла. Конструкция принятия двоичного решения IF-THEN-ELSE. Преимущества использования модульного принципа.

Корректность реализации и верификация информационных (автоматизированных) систем. Понятие корректности или правильности проверяемого объекта. Спецификация требований программного обеспечения. Функциональные критерии и характеристики. Неформализованные представления разработчика. Спецификация требований программного обеспечения (Software Requirements Specification).

Представления функциональных требований. Рекомендации к структуре и методам описания программных требований. Основные ключевые требования «хорошей спецификации». Требования к программной спецификации. Основные подходы к определению спецификаций требований.

Теория безопасных систем (ТСВ). Понятие «доверенная вычислительная среда» (trusted computing base-TCB). Дискретная природа характеристики «безопасный». Характеристика «доверенный». Доверенная вычислительная среда. Набор компонентов, составляющий доверенную вычислительную среду. Этапы разработки защищённой АС. Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2000). Цель создания АСЗИ.

Тема № 9. Общие сведения о стандартах в области информационной безопасности

Понятие стандарта в области информационной безопасности (ИБ). Обоснование необходимости использования стандартов в области ИБ. Главная задача стандартов в области ИБ. Стандарты как основной механизм обеспечения совместимости продуктов и систем. Основы взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий (ИТ). Регламентация необходимости применения средств, механизмов, алгоритмов. Требования безопасности.

Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.

Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.

Набор требований к подсистемам защиты АС. Проверка соответствия требованиям по защите информации от НСД для АС. Показатели защищённости от НСД к информации в АС.

Стандарт «Критерии оценки доверенных компьютерных систем»/ TCSEC («Оранжевая книга»). Цель разработки стандарта TCSEC. Требования безопасности, предъявляемых к аппаратному, программному и специальному

обеспечению компьютерных систем. Категории требований безопасности. Общая структура требований к системам защиты.

Политика безопасности. Возможность осуществления субъектами доступа к объектам. Разграничение доступа к категорированной информации. Метки безопасности как механизм контроля доступа.

Аудит. Идентификация и аутентификация. Механизм защиты данных. Регистрация и учёт. Корректность. Контроль корректности функционирования средств защиты. Непрерывность защиты.

Основные положения «Общих критериев». Свойство «Общих критериев». Структура «Общих критериев». Определение объекта оценки и продукта. Система как специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

Категории пользователей. Среда безопасности. Задачи, решаемые при подготовке к оценке. Требования по безопасности. Каталоги требований безопасности. Общая модель безопасности. Недостатки «Общих критериев».

Профили защиты. Введение профиля защиты. Идентификация профиля защиты. Аннотация профиля защиты. Описание объекта оценки. Характерные особенности ИТ применительно к объекту оценки (ОО).

Среда безопасности ОО. Описание аспектов безопасности среды, в которой предполагается использовать ОО. Структура и содержание профиля защиты. Цели безопасности для ОО. Цели безопасности для среды ОО.

Функциональные требования и требования доверия. Основные осуществляемые операции при выборе компонентов функциональных требований. Требования доверия к безопасности ОО. Обоснование профиля защиты.

Тема № 10. Концепция защиты СВТ и АС от НСД в соответствии с руководящими документами Гостехкомиссии и нормативно-методическими документами ФСТЭК России

Перечень основных документов ФСТЭК РФ по вопросам защиты информации. Основные положения концепции защиты СВТ и АС от НСД к информации. Определение НСД к информации. Два направления защиты от НСД. Особенности функций защиты в СВТ и АС. Основные способы НСД. Принципы защиты от НСД. Построение модели нарушителя безопасности АС. Уровни возможностей, предоставляемые нарушителям штатными средствами АС и СВТ. Характеристики оценки технических средств защиты от НСД. Система разграничения доступа (СРД) и её функции. Средства для СРД. Реализация СРД. Проверка выполнения технических требований по защите. Сертификат соответствия СВТ или АС требованиям по защите.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине (модулю).

«Методические указания для обучающихся по освоению дисциплины (модуля)» представлены в Приложении 2 к настоящей РП.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине (модулю) «Теоретические основы компьютерной безопасности» приведена в Приложении 1 к настоящей РП.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основнаялитература:

1.Гагарина Л.Г., Федоров А.Р., Федоров П.А. Введение в архитектуру программного обеспечения: Учебное пособие - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 320 с. ISBN 978-5-8199-0649-1. / ЭБС «Знаниум» http://znanium.com/bookread2.php?book=542665

2.Астапчук В.А., Терещенко П.В. Архитектура корпоративных информационных систем – Новосиб.: НГТУ, 2015. - 75 с.: ISBN 978-5-7782-2698-2. / ЭБС «Знаниум» http://znanium.com/bookread2.php?book=546624

Дополнительная литература:

3.Царев Р.Ю., Прокопенко А.В., Князьков А.Н. Программные и аппаратные средства информатики - Краснояр.: СФУ, 2015. - 160 с. ISBN 978-5-7638-3187-0 / ЭБС «Знаниум» http://znanium.com/bookread2.php?book=550017

4.Дворовенко, О. В. Информационно-аналитические продукты и услуги: практикум по направлению подготовки 51.03.06 «Библиотечно-информационная деятельность», профиль подготовки «Информационно-аналитическая деятельность», квалификация (степень) выпускника: «бакалавр» : учебное пособие / О. В. Дворовенко. — Кемерово : КемГИК, 2021. — 54 с. — ISBN 978-5-8154-0604-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/250628 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
ЭБС Лань (lanbook.com)

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Интернет-ресурсы:

1. **http://www.gov.ru** - сервер органов государственной власти Российской Федерации.
2. **http://www.minfin.ru** - официальный сайт Министерства финансов Российской Федерации.
3. http://www.biblioclub.ru
4. http://znanium.com
5. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации

6. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности
7. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

9. Методические указания для обучающихся, по освоению дисциплины (модуля)

Методические указания для обучающихся, по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модуля)

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**
  1.Электронные ресурсы образовательной среды университета
  2.Информационно-справочные системы:
  Консультант+; Гарант

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7; программы эмуляции виртуальных машин (VM-vare, VM-box или др.); операционная система MS Windows Server 2003 или др. сетевая ОС.
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Лабораторные работы:

- компьютерная аудитория, оснащенная программно-аппаратными средствами защиты информации и аудита компьютерной безопасности, а также оснащенная специализированным оборудованием и контрольно-измерительной аппаратурой.

Самостоятельная работа студентов может проводится как в специально оборудованных компьютерных классах университета с выходом в Интернет, так и в домашних условиях при наличии Интернет – сети.

Задания:

ЗАДАНИЕ № 1

Тема: Теоретические аспекты проведения специальных исследований (СИ) на предприятии

Цель работы.

Изучение основных принципов проведения специальных исследований на предприятии. Освоить структуру ведения общей теоретической части проведения специальных исследований.

Продолжительность занятия: полтора учебных часа.

Задания.

1. Изучить теоретическую часть Задания №1.
2. Выполнить практическую часть Задания №1:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

3. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Специальные исследования (специсследования, СИ) — комплекс действий, направленный на обнаружение потенциальных технических каналов утечки защищаемой информации с помощью специального контрольно-измерительного оборудования, в соответствии с нормативно-методическими документами ФСБ России и ФСТЭК России.

Проведение специсследований определяет возможность считывания и перехвата сигнала специальными средствами разведки в рамках определённых границ (защищённость утечек по каналам ПЭМИН — побочные электромагнитные излучения и наводки).

Введем для большей ясности определения, связанные с основой ведения специсследований на предприятии. Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается ценная информация.

Автоматизированная система (АС) – устройство или комплекс устройств, необходимых для передачи, хранения и обработки конфиденциальной информации, прошедшая процедуру аттестации в соответствии с законодательством РФ.

Контролируемая зона (КЗ) – пространство, в котором исключено неконтролируемое пребывание посторонних лиц или сотрудников, не имеющих прямое отношение к данному пространству. Примерами могут послужить: периметр охраняемой территории; ограждающие конструкции охраняемого здания или охраняемой территории.

Информационный сигнал – электрические сигналы, акустические, электромагнитные и т.д., по параметрам которых можно раскрыть конфиденциальную информацию, передаваемую, хранимую или обрабатываемую в основных технических средствах и системах или обсуждаемая в защищенном исполнении.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для обработки, хранения и передачи конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

Средства активной защиты информации по каналам ПЭМИН (САЗ) – технические средства формирования маскирующих электромагнитных помех

в местах возможного съема защищаемой информации, прошедшие обязательную процедуру сертификации по линии ФСТЭК России.

Деятельность по технической защите конфиденциальной информации (ТЗКИ) – выполнение работ и (или) оказание услуг по ее защите:

– от несанкционированного доступа,

– от утечки по техническим каналам,

– от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Важно! Данный вид деятельности является лицензируемым. Лицензирование деятельности по ТЗКИ осуществляет ФСТЭК России.

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные поля, создаваемые в окружающем пространстве СВТ, специально для этого не предназначенными (в случае ПЭМИ) или наводки данных излучений на токоведущие конструкции, линии и подключенные к ним ТС.

Существует несколько видов проведения специсследований на определенные ТС. В данном случае это акустоэлектрическое преобразование (АЭП) и ПЭМИН. В случае АЭП исследуемое средство подвергается воздействию некоих акустических частот. Из этого обосновывается определенный вывод о возможности использования ТС на невозможности подверженности АЭП.

Как уже было указано в определениях, ПЭМИ создаются вокруг работающих технических средств, которые специально для данного излучения не создавались. То есть излучение от радиопередатчиков, мобильных телефонов – это не побочные излучения. А вот излучения при работе компьютера от монитора, принтера, накопителей информации являются побочными.

Если вспомнить физику, то вокруг проводника, по которому протекает электрический ток возникает электромагнитное поле. Если по данному проводнику передается какой-либо сигнал, то, следовательно, и электромагнитное поле тоже будет изменяться по тем же законам, что и сигнал, протекающий в линии. Таким образом, источником сигнала ПЭМИ являются все токо-

ведущие линии в ТС, по которым в процессе работы передаются какие-либо сигналы.

Как известно электромагнитные поля могут распространяться на значительные расстояния и конструкции помещений тому не преграда. Скорость передачи данных и обработки информации в современных средствах вычислительной техники постоянно растет, а значит растут и частоты сигналов ПЭМИ. Частоты сигналов ПЭМИ могут начинаться от единиц кГц и заканчиваться единицами ГГц, а гармоники этих сигналов могут находиться еще выше по частоте.

Если вспомнить, что в проводнике, помещенном в электромагнитное поле, возникает электрический ток, то очевидно, что могут возникать наводки ПЭМИ на любые токоведущие элементы (систему отопления, короб системы вентиляции и т. д.), в том числе и любые линии и ТС, подключенные к ним, попадающие под действие данного электромагнитного поля.

Перехват этой информации можно осуществить путем анализа изменений параметров ПЭМИН с помощью специальных высокочувствительных радиоприемных устройств, оснащенных специализированными антеннами, пробниками напряжения, токосъемниками.

На (рис. 1) приведена физика утечки информации за счет ПЭМИ.

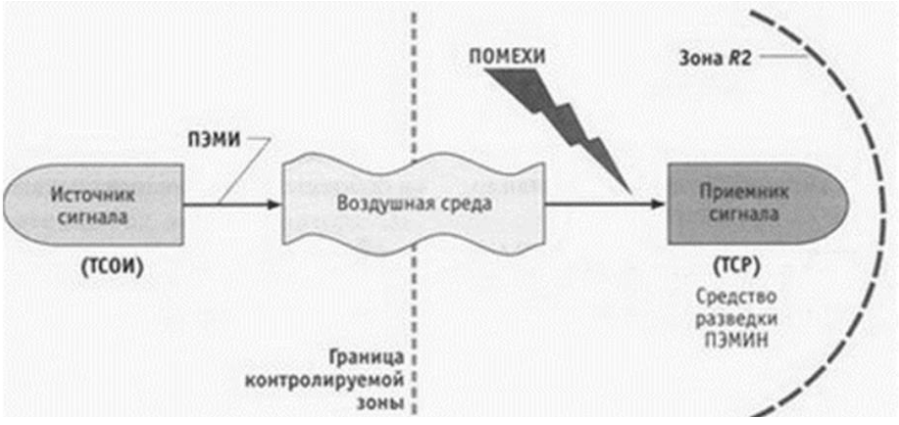


Рисунок 1. Схема ТКУИ за счет ПЭМИ

На (рис. 2) приведена физика утечки информации за счет ПЭМИН.

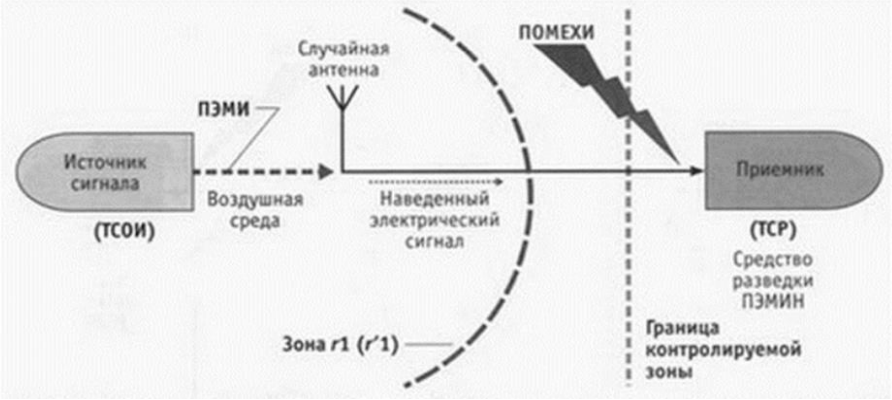


Рисунок 2. Схема ТКУИ за счет ПЭМИН

Поясним некоторые сокращения и термины на схемах:

- ТСОИ – технические средства обработки информации (все что попадает под определение ОТСС);
- ТСР–технические средства разведки;
- зона R2 – расстояние, на котором возможен перехват защищаемой информации за счет ПЭМИ;
- зона r1(r'1) – расстояние, наличие в пределах которого случайных антенн (токоведущие конструкции, линии и ТС) создает возможность утечки информации за счет наводок ПЭМИ.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенной случайной антенной может являться стационарный телефон, датчик пожарной сигнализации, громкоговоритель, подключенная к линии, выходящей за пределы КЗ.

Распределенные случайные антенным – антенны с распределенными параметрами. К ним можно отнести: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ.

Также разделяют саму информации по каналам АЭП и ПЭМИ на случай информативности. Информативные – сигналы с несущей, модулированной информативным сигналом. Примером могут послужить: сигнал от флэш-накопителя USB; VGA-интерфейс монитора; и т.д.

Неинформативные сигналы – сигналы, анализ которых не дает представления об обрабатываемой информации. Примеры: излучения от работы

источников питания в узлах ТС; сигнал обработки режимов видеокартой; и т.д.

Важно! Всё приведенное выше относится к составной части по проведению работ, связанных с специальными исследованиями ОТСС и ВТСС. Однако это лишь малая часть того, что можно было бы изложить. Остальная теоретическая и прикладная часть изучается непосредственно работником предприятия в режимно секретном подразделении. Все методические материалы работ, связанных с проведением специальных исследований имеют грифы СЕКРЕТНО и СОВЕРШЕННО СЕКРЕТНО. Вышеизложенный материал является открытым и считается опорным в общих знаниях ТЗИ.

Практическая часть.

Вопросы для самопроверки:

1) Дайте определение специальным исследованиям в рамках данного учебного занятия.
2) Какие и сколько существует грифов секретности в рамках законодательства РФ?
3) Что такое зона r1(r'1) в ТЗИ?
4) Дайте определение ОТСС и ВТСС и в чем их различие?
5) На какие категории разбиваются случайные антенны в КЗ и в чем их разница? И на какие категории разбиваются информационные сигналы и в чем их разница?

Практические задания:

1) Опишите собственными словами следующие определения. ОТСС; ВТСС; ТКУИ.
2) В соответствии с (рис. 1) данного учебного задания, источником распространения сигнала ПЭМИ между техническим средством и техническим средством разведки является воздушная среда. Что бу-

дет если изменить воздушную среду на более плотную, а что, если перенести её в вакуум. Ответ обоснуйте.

Однажды, двое ученых задались очень интересной задачей, связанной с передачей информативного сигнала технического средства через канал ПЭМИ по очень интересной схеме. У них получилось и даже на современном этапе злоумышленники охотно придают значение данному средству получения заведомо важной для них информации. Двух ученых звали Маркус Кун и Росс Андерсон. При помощи сети Интернет, найдите информацию о данной процедуре получения информативного сигнала по каналу ПЭМИ и расскажите в общих чертах об этой технологии

ЗАДАНИЕ № 2

Тема: Теоретические основы средств измерения программно-аппаратных комплексов (ПАК) и альтернативной измерительной площадки (АИП)

Цель работы.

Изучение теоретической основы средств измерений сигналов. Освоить особенности поиска и идентификации сигналов при помощи альтернативной измерительной площадки.

Продолжительность занятия: полтора учебных часа.

Задания.

4. Изучить теоретическую часть Задания №2.
5. Выполнить практическую часть Задания №2:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

6. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

В связи с тем, что многие организации, занимающиеся производством и распространением программно-аппаратных комплексов, предлагают на рынке целые линейки своих продуктов, отличающихся только аппаратной частью (анализаторы спектра) и соответственно ценой на данные товары в этой линейке. На рынке представлены программ- но-аппаратные комплексы следующих производителей, распространителей: «Навигатор ПхГ» – «НЕЛК», «Сигурд Мх» – «МАСКОМ», «Легенда» – «АВМ-СИСТЕМС». Стоит отметить, что все комплексы, рассматриваемые в данной работе, имеют сертификаты ФСТЭК России и метрологический сертификат соответствия на измерительное оборудование. Пример ПАК представлен на (рис. 1).

Рисунок 1. ПАК «Сигурд М18»

Требования к антеннам.

В полосе частот от 200 Гц до 30 МГц в комплект антенн должны входить магнитная и (или) электрическая антенны.

Для измерения магнитной составляющей электромагнитного поля, антенна должна быть: электрически экранированной рамочной антенной, имеющей такие размеры, чтобы ее рамка помещалась в квадрат со стороной не более 0,6 м, или ферритовая антенна длиной не более 0,5 м.

Допускаемая погрешность измерений напряженности магнитного поля (измеритель с магнитной антенной) не должна превышать 2,5 дБ.

Конструкция антенн (антенного штатива) должна обеспечивать возможность плавного изменения высоты расположения антенны над землей от 0,8 м до 1,25 м, а также возможность поворота магнитной и электрической антенн на 360° вокруг оси.

В полосе частот от 30 до 1000 МГц в комплект антенн должны входить одна или несколько электрических антенн одного из следующих типов:

а) линейный симметричный вибратор на полосу частот от 30 до 80 МГц, размер которого равен длине полуволнового симметричного вибратора на частоте 80 МГц, и настраиваемый полуволновой симметричный вибратор в полосе частот от 80 до 1000 МГц, имеющий КСВН не более 2,5;

б) биконическая антенна, максимальный размер которой должен быть не более 1,35 м в полосе частот от 30 до 300 МГц и с КСВН не более 3,0, и биконическая антенна, максимальный размер которой – не более 0,5 м в полосе частот от 300 до 1000 МГц с КСВН не более 2,5;

в) широкополосная антенна, главный лепесток диаграммы направленности которой должен быть таким, чтобы в направлении непосредственного излучения от источника ПЭМИН и в направлении отраженного от земли луча разность коэффициентов усиления антенны не превышала бы 1 дБ, с КСВН не более 2,5.

Конструкция антенны (антенного штатива) должна обеспечивать возможность плавного изменения высоты центра симметрии над землей от 1 до 4 м и поворота вокруг горизонтальной оси на 180°, а также фиксированную ориентацию в трех взаимно ортогональных направлениях.

Допускаемая погрешность измерений напряженности электрического поля (измеритель с биконической, электрической антенной) не должна превышать 2,5 дБ на частотах до 1000 МГц.

Антенны должны иметь коэффициент калибровки, позволяющий измерять уровни полей. Рекомендуемый коэффициент калибровки антенн – не

более 40 дБ. Погрешность коэффициента калибровки антенн должна быть не более 2 дБ.

Требования к анализатору.

Должен иметь несимметричный вход с номинальным значением сопротивления 50 Ом с коэффициентом стоячей волны по напряжению (КСВН) не более 2 при ослаблении входного аттенюатора 0 дБ и не более 1,2 при ослаблении входного аттенюатора 10 дБ и более.

Измерители совместно с первичными преобразователями должны обеспечивать измерения характеристик ПЭМИ в децибелах, относительно 1 мкВ, 1 мкА, 1 мкВ/м, 1 мкА/м, 1 мВт/м2.

Анализатор спектра должен быть программируемым, для дистанционного управления, т. е. должен обрабатывать команды, которые ему посылает ПЭВМ.

Должен иметь интерфейсы LAN или USB, или GPIB, или RS-232 для передачи данных с ПЭВМ на анализатор спектра и обратно.

Анализатор спектра должен иметь квазипиковый, пиковый и со среднеквадратичным отклонением детекторы.

Работать в полосе частот 9 кГц...1000 МГц.

Иметь полосы пропускания в диапазоне 1 кГц...3 МГц. Погрешность, вносимая собственными шумами, должна быть не более 1 дБ. Анализатор спектра должен обеспечивать звуковой контроль ПЭМИ, имеющих амплитудную и частотную (на частотах свыше 30 МГц) модуляцию, с помощью встроенных или подключаемых приборов или устройств.

Примерный перечень оборудования приведен в (табл. 1).

Таблица 1. Перечень оборудования для проведения оценки защищенности по каналу ПЭМИН

Наименование средств измерения	Тип	Диапазон частот
Анализатор спектра	LIGNext1 NS-30A	10 кГц -3 ГГц
Антенна магнитная рамочная активная	Н-30	10 Гц – 30 МГц
Антенна электрическая дипольная активная	Е-3000	30 МГц – 3000 МГц
Антенна электрическая дипольная активная	Е-30	10 Гц – 30 МГц
Пробник напряжения	П-400	10 Гц – 300 МГц
Осциллограф	LeCroy Wavesurfer 62Xs	0 Гц – 600 МГц
Генератор сигналов	Г4-218	200 кГц-1 ГГц

Альтернативная измерительная площадка.

Временная методика оценки защищенности ОТСС, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации (КИ), описанная в «Сборнике временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам» предполагает собой поиск и измерение опасных сигналов непосредственно на объекте информатизации.

Однако, шумовая обстановка на объекте информатизации весьма нестабильна. Помимо нестабильности она абсолютно неисследованная. Оператор при проведении измерений может столкнуться с таким явлением как «стоячая волна».

Стоячая волна (электромагнитная) – периодическое изменение амплитуды напряженности электрического и магнитного полей вдоль направления распространения, вызванное интерференцией, падающей и отраженной волн. Например, стоячая волна возникает при отражении волны от преград и неод-

нородностей в результате взаимодействия (интерференции), падающей и отражённой волн.

Присутствие такой волны во время проведения измерений однозначно приведёт к ошибке.

Измерительная площадка – площадка, отвечающая требованиям, обеспечивающим правильное измерение уровней индустриальных радиопомех (ИРП), излучаемых ТС в регламентированных условиях. Видов ИП предусматриваются два – «открытая измерительная площадка» и «альтернативная измерительная площадка». Поскольку строительство и эксплуатация открытой площадки весьма дорого, сосредоточимся на более дешёвом варианте – АИП. Разница между открытой ИП и АИП заключается в том, что последняя должна размещаться не в открытом пространстве, а в некотором помещении, в здании. При том физические характеристики АИП (прежде всего «затухание» электромагнитного поля) должны оставаться в пределах установленного допуска.

Важно! Перед вводом в эксплуатацию АИП оценивается минимум искажений, вносимых в распределение электромагнитного поля ограждающими конструкциями помещения, который можно допустить. Иными словами, оператор заранее знает о наличии и характере «стоячих волн» и о характеристиках закона затухания электромагнитного поля. Это позволяет получать информацию об «опасных» информативных сигналах корректнее, чем на ОИ, на котором абсолютно не исследована шумовая обстановка.

Практическая часть.

Вопросы для самопроверки:

1) Назовите весь перечень оборудования для проведения оценки защищенности по ПЭМИ.
2) Дайте определение измерительной площадки в рамках данного задания.

3) Сколько существует видов измерительных площадок (ИП) и в чем их различие?
4) На сколько метров минимально и максимально предполагается плавное размещение антенны по высоте?
5) Какой должен быть коэффициент калибровки у антенн?

Практические задания:

1) Как по Вашему мнению вы представляете себе открытую измерительную площадку и альтернативную? Опишите их. В чем их основное различие? Ответ обоснуйте.
2) Представьте, что Вы начинающий сотрудник предприятия ООО «НПП «ИБЦ». Начался ваш седьмой рабочий день. Вы в обычном распорядке, получив задание, идете включать лабораторное автоматизированное рабочее место и ПАК. Неожиданным образом узнаёте, что откалиброванная антенна начала давать сбой. Вы (без особой паники) начинаете искать пути решения. По Вашему мнению, каковы основные три шага на пути решения этой проблемы? Ответ обоснуйте.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль: Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1.Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию управления действий.	Тема:1-5	УК-1.3 Использует методы системного и критического анализа, анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.	УУК-1.2. Определяет уязвимости и угрозы информационной безопасности, необходимые для выявления и решения проблемной ситуации, планирует мероприятия и процессы по их устранению на основе системного и междисциплинарных подходов.	УК-1.1. Ставит цель, определяет способы ее достижения, разрабатывает стратегию действия, принимает конкретные решения для ее реализации с учетом требований регуляторов в области защиты информации
2.	ПК-3	Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности.	Тема:1-5	ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.	ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.	ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

Код компетенции	Инструменты, оценивающие сформированность компетенции	***Этапы и показатель оценивания компетенции***	***Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания***
УК-1 ПК-3	***Тест***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	***Например:*** ***Проводится письменно. Время, отведенное на процедуру - 30 минут.*** ***Неявка – 0 баллов.*** ***Критерии оценки определяются процентным соотношением.*** ***Неудовлетворительно – менее 50% правильных ответов.*** ***Удовлетворительно - от 51% правильных ответов.*** ***Хорошо - от 70%.*** ***Отлично – от 90%.*** ***Максимальная оценка – 5 баллов.***
УК-1 ПК-3	Доклад	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
УК-1 ПК-3	Контрольная работа	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция***	1. Проводится устно в форме защиты отчета 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие оформления требованиям (1 балл). 2. Соответствие разработанного устрой-

Код компетенции	Инструменты, оценивающие сформированность компетенции	***Этапы и показатель оценивания компетенции***	***Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания***
		освоена на базовом уровне – 3 балла; ***В) не сформирована (компетенция не сформирована) – 2 и менее баллов***	ства техническому заданию (1 балл) 3. Моделирование работы разработанного устройства (1 балл) 4. Качество и количество используемых источников (1 балл) 5. Правильность и полнота ответов на контрольные вопросы (1 балл) Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал.
УК-1 ПК-3	***Лабораторная работа***	***А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на продвинутом уровне – 4 балла;*** • ***компетенция освоена на базовом уровне – 3 балла;*** ***В) не сформирована (компетенция не сформирована) – 2 и менее баллов***	***1. Оформление в соответствии с требованиями (1 балл).*** ***2. Выбор методов измерений и вычислений (1 балл).*** ***3. Умение применять выбранные методы (1 балл).*** ***4. Анализ и выводы, отражающие суть изучаемого явления с указанием конкретных результатов (2 балла).*** ***Максимальная оценка – 5 баллов.***

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

.Примерная тематика докладов в форме презентаций:

1. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности. Основы обеспечения безопасности информации в компьютерных системах.
2. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного получения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям.
3. Проектирование архитектуры системы защиты информации выбранного объекта и оценка его уровня защищённости.

4. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.

5. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации.

6. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию.

7. Направления повышения эффективности существующей системы защиты и методика применения средств защиты информации на выбранных объектах исследования.

8. Разработка проекта создания системы защиты информации на выбранных типовых офисных объектах.

9. Основные виды атак на компьютерные системы (КС), их классификация, проблемы обеспечения информационной безопасности в проводных КС.

10. Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.

11. Компьютерная преступность в экономических областях.

12. Компьютерные вирусы в современных информационных системах.

13. Информационные угрозы современным экономическим объектам.

14. Безопасность информации в коммерческой деятельности.

15. Становление и развитие промышленного шпионажа.

16. Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.

17. Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU).

18. Направления повышения эффективности существующей системы защиты и методика применения средств защиты информации на выбранных объектах исследования.

19. Общий подход к построению систем, реализующих мандатную (полномочную) политику безопасности в модели BL (Белла-Лападулы).

20. Назначение модели Белла-Лападулы. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы.

Примерная тематика (контрольных заданий) задач для выполнения:

ЗАДАНИЕ № 1

Тема: Теоретические аспекты проведения специальных исследований (СИ) на предприятии

Цель работы.

Изучение основных принципов проведения специальных исследований на предприятии. Освоить структуру ведения общей теоретической части проведения специальных исследований.

Продолжительность занятия: полтора учебных часа.

Задания.

7. Изучить теоретическую часть Задания №1.
8. Выполнить практическую часть Задания №1:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

9. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Специальные исследования (специсследования, СИ) — комплекс действий, направленный на обнаружение потенциальных технических каналов утечки защищаемой информации с помощью специального контрольно-измерительного оборудования, в соответствии с нормативно-методическими документами ФСБ России и ФСТЭК России.

Проведение специсследований определяет возможность считывания и перехвата сигнала специальными средствами разведки в рамках определён-

ных границ (защищённость утечек по каналам ПЭМИН — побочные электромагнитные излучения и наводки).

Введем для большей ясности определения, связанные с основой ведения специсследований на предприятии. Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается ценная информация.

Автоматизированная система (АС) – устройство или комплекс устройств, необходимых для передачи, хранения и обработки конфиденциальной информации, прошедшая процедуру аттестации в соответствии с законодательством РФ.

Контролируемая зона (КЗ) – пространство, в котором исключено неконтролируемое пребывание посторонних лиц или сотрудников, не имеющих прямое отношение к данному пространству. Примерами могут послужить: периметр охраняемой территории; ограждающие конструкции охраняемого здания или охраняемой территории.

Информационный сигнал – электрические сигналы, акустические, электромагнитные и т.д., по параметрам которых можно раскрыть конфиденциальную информацию, передаваемую, хранимую или обрабатываемую в основных технических средствах и системах или обсуждаемая в защищенном исполнении.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для обработки, хранения и передачи конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

Средства активной защиты информации по каналам ПЭМИН (САЗ) – технические средства формирования маскирующих электромагнитных помех в местах возможного съема защищаемой информации, прошедшие обязательную процедуру сертификации по линии ФСТЭК России.

Деятельность по технической защите конфиденциальной информации (ТЗКИ) – выполнение работ и (или) оказание услуг по ее защите:

– от несанкционированного доступа,

– от утечки по техническим каналам,

– от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Важно! Данный вид деятельности является лицензируемым. Лицензирование деятельности по ТЗКИ осуществляет ФСТЭК России.

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные поля, создаваемые в окружающем пространстве СВТ, специально для этого не предназначенными (в случае ПЭМИ) или наводки данных излучений на токоведущие конструкции, линии и подключенные к ним ТС.

Существует несколько видов проведения специсследований на определенные ТС. В данном случае это акустоэлектрическое преобразование (АЭП) и ПЭМИН. В случае АЭП исследуемое средство подвергается воздействию некоих акустических частот. Из этого обосновывается определенный вывод о возможности использования ТС на невозможности подверженности АЭП.

Как уже было указано в определениях, ПЭМИ создаются вокруг работающих технических средств, которые специально для данного излучения не создавались. То есть излучение от радиопередатчиков, мобильных телефонов – это не побочные излучения. А вот излучения при работе компьютера от монитора, принтера, накопителей информации являются побочными.

Если вспомнить физику, то вокруг проводника, по которому протекает электрический ток возникает электромагнитное поле. Если по данному проводнику передается какой-либо сигнал, то, следовательно, и электромагнитное поле тоже будет изменяться по тем же законам, что и сигнал, протекаю-

щий в линии. Таким образом, источником сигнала ПЭМИ являются все токоведущие линии в ТС, по которым в процессе работы передаются какие-либо сигналы.

Как известно электромагнитные поля могут распространяться на значительные расстояния и конструкции помещений тому не преграда. Скорость передачи данных и обработки информации в современных средствах вычислительной техники постоянно растет, а значит растут и частоты сигналов ПЭМИ. Частоты сигналов ПЭМИ могут начинаться от единиц кГц и заканчиваться единицами ГГц, а гармоники этих сигналов могут находиться еще выше по частоте.

Если вспомнить, что в проводнике, помещенном в электромагнитное поле, возникает электрический ток, то очевидно, что могут возникать наводки ПЭМИ на любые токоведущие элементы (систему отопления, короб системы вентиляции и т. д.), в том числе и любые линии и ТС, подключенные к ним, попадающие под действие данного электромагнитного поля.

Перехват этой информации можно осуществить путем анализа изменений параметров ПЭМИН с помощью специальных высокочувствительных радиоприемных устройств, оснащенных специализированными антеннами, пробниками напряжения, токосъемниками.

На (рис. 1) приведена физика утечки информации за счет ПЭМИ.

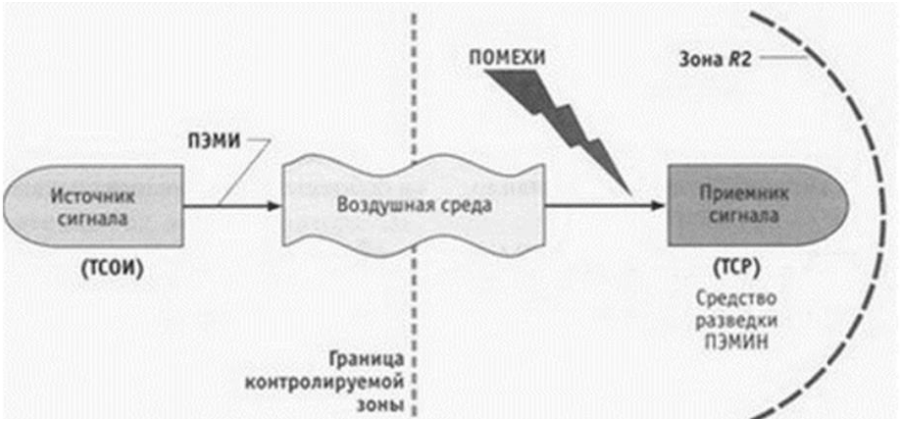


Рисунок 1. Схема ТКУИ за счет ПЭМИ

На (рис. 2) приведена физика утечки информации за счет ПЭМИН.

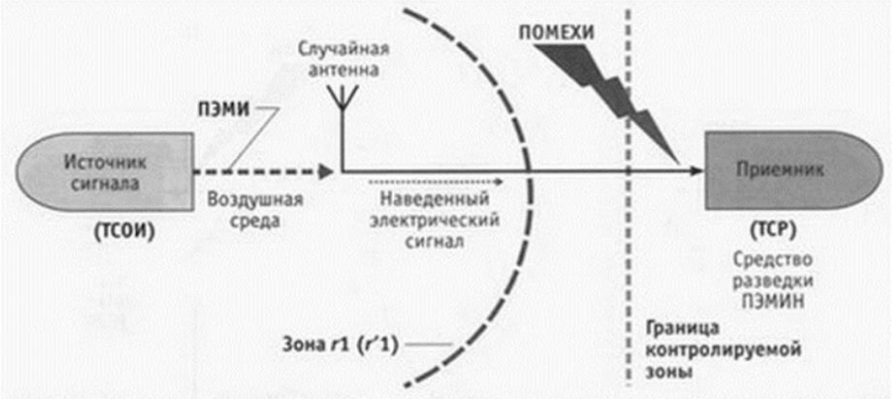


Рисунок 2. Схема ТКУИ за счет ПЭМИН

Поясним некоторые сокращения и термины на схемах:

- ТСОИ – технические средства обработки информации (все что попадает под определение ОТСС);
- ТСР–технические средства разведки;
- зона R2 – расстояние, на котором возможен перехват защищаемой информации за счет ПЭМИ;
- зона r1(r'1) – расстояние, наличие в пределах которого случайных антенн (токоведущие конструкции, линии и ТС) создает возможность утечки информации за счет наводок ПЭМИ.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенной случайной антенной может являться стационарный телефон, датчик пожарной сигнализации, громкоговоритель, подключенная к линии, выходящей за пределы КЗ.

Распределенные случайные антенным – антенны с распределенными параметрами. К ним можно отнести: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ.

Также разделяют саму информации по каналам АЭП и ПЭМИ на случай информативности. Информативные – сигналы с несущей, модулированной информативным сигналом. Примером могут послужить: сигнал от флэш-накопителя USB; VGA-интерфейс монитора; и т.д.

Неинформативные сигналы – сигналы, анализ которых не дает представления об обрабатываемой информации. Примеры: излучения от работы

источников питания в узлах ТС; сигнал обработки режимов видеокартой; и т.д.

Важно! Всё приведенное выше относится к составной части по проведению работ, связанных с специальными исследованиями ОТСС и ВТСС. Однако это лишь малая часть того, что можно было бы изложить. Остальная теоретическая и прикладная часть изучается непосредственно работником предприятия в режимно секретном подразделении. Все методические материалы работ, связанных с проведением специальных исследований имеют грифы СЕКРЕТНО и СОВЕРШЕННО СЕКРЕТНО. Вышеизложенный материал является открытым и считается опорным в общих знаниях ТЗИ.

Практическая часть.

Вопросы для самопроверки:

6) Дайте определение специальным исследованиям в рамках данного учебного занятия.
7) Какие и сколько существует грифов секретности в рамках законодательства РФ?
8) Что такое зона r1(r'1) в ТЗИ?
9) Дайте определение ОТСС и ВТСС и в чем их различие?
10) На какие категории разбиваются случайные антенны в КЗ и в чем их разница? И на какие категории разбиваются информационные сигналы и в чем их разница?

Практические задания:

3) Опишите собственными словами следующие определения. ОТСС; ВТСС; ТКУИ.
4) В соответствии с (рис. 1) данного учебного задания, источником распространения сигнала ПЭМИ между техническим средством и техническим средством разведки является воздушная среда. Что бу-

дет если изменить воздушную среду на более плотную, а что, если перенести её в вакуум. Ответ обоснуйте.

Однажды, двое ученых задались очень интересной задачей, связанной с передачей информативного сигнала технического средства через канал ПЭМИ по очень интересной схеме. У них получилось и даже на современном этапе злоумышленники охотно придают значение данному средству получения заведомо важной для них информации. Двух ученых звали Маркус Кун и Росс Андерсон. При помощи сети Интернет, найдите информацию о данной процедуре получения информативного сигнала по каналу ПЭМИ и расскажите в общих чертах об этой технологии

ЗАДАНИЕ № 2

Тема: Теоретические основы средств измерения программно-аппаратных комплексов (ПАК) и альтернативной измерительной площадки (АИП)

Цель работы.

Изучение теоретической основы средств измерений сигналов. Освоить особенности поиска и идентификации сигналов при помощи альтернативной измерительной площадки.

Продолжительность занятия: полтора учебных часа.

Задания.

10. Изучить теоретическую часть Задания №2.
11. Выполнить практическую часть Задания №2:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

12. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

В связи с тем, что многие организации, занимающиеся производством и распространением программно-аппаратных комплексов, предлагают на рынке целые линейки своих продуктов, отличающихся только аппаратной частью (анализаторы спектра) и соответственно ценой на данные товары в

этой линейке. На рынке представлены программ- но-аппаратные комплексы следующих производителей, распространителей: «Навигатор ПхГ» – «НЕЛК», «Сигурд Мх» – «МАСКОМ», «Легенда» – «АВМ-СИСТЕМС». Стоит отметить, что все комплексы, рассматриваемые в данной работе, имеют сертификаты ФСТЭК России и метрологический сертификат соответствия на измерительное оборудование. Пример ПАК представлен на (рис. 1).

Рисунок 1. ПАК «Сигурд М18»

Требования к антеннам.

В полосе частот от 200 Гц до 30 МГц в комплект антенн должны входить магнитная и (или) электрическая антенны.

Для измерения магнитной составляющей электромагнитного поля, антенна должна быть: электрически экранированной рамочной антенной, имеющей такие размеры, чтобы ее рамка помещалась в квадрат со стороной не более 0,6 м, или ферритовая антенна длиной не более 0,5 м.

Допускаемая погрешность измерений напряженности магнитного поля (измеритель с магнитной антенной) не должна превышать 2,5 дБ.

Конструкция антенн (антенного штатива) должна обеспечивать возможность плавного изменения высоты расположения антенны над землей от

0,8 м до 1,25 м, а также возможность поворота магнитной и электрической антенн на 360° вокруг оси.

В полосе частот от 30 до 1000 МГц в комплект антенн должны входить одна или несколько электрических антенн одного из следующих типов:

а) линейный симметричный вибратор на полосу частот от 30 до 80 МГц, размер которого равен длине полуволнового симметричного вибратора на частоте 80 МГц, и настраиваемый полуволновой симметричный вибратор в полосе частот от 80 до 1000 МГц, имеющий КСВН не более 2,5;

б) биконическая антенна, максимальный размер которой должен быть не более 1,35 м в полосе частот от 30 до 300 МГц и с КСВН не более 3,0, и биконическая антенна, максимальный размер которой – не более 0,5 м в полосе частот от 300 до 1000 МГц с КСВН не более 2,5;

в) широкополосная антенна, главный лепесток диаграммы направленности которой должен быть таким, чтобы в направлении непосредственного излучения от источника ПЭМИН и в направлении отраженного от земли луча разность коэффициентов усиления антенны не превышала бы 1 дБ, с КСВН не более 2,5.

Конструкция антенны (антенного штатива) должна обеспечивать возможность плавного изменения высоты центра симметрии над землей от 1 до 4 м и поворота вокруг горизонтальной оси на 180°, а также фиксированную ориентацию в трех взаимно ортогональных направлениях.

Допускаемая погрешность измерений напряженности электрического поля (измеритель с биконической, электрической антенной) не должна превышать 2,5 дБ на частотах до 1000 МГц.

Антенны должны иметь коэффициент калибровки, позволяющий измерять уровни полей. Рекомендуемый коэффициент калибровки антенн – не более 40 дБ. Погрешность коэффициента калибровки антенн должна быть не более 2 дБ.

Требования к анализатору.

Должен иметь несимметричный вход с номинальным значением сопротивления 50 Ом с коэффициентом стоячей волны по напряжению (КСВН) не более 2 при ослаблении входного аттенюатора 0 дБ и не более 1,2 при ослаблении входного аттенюатора 10 дБ и более.

Измерители совместно с первичными преобразователями должны обеспечивать измерения характеристик ПЭМИ в децибелах, относительно 1 мкВ, 1 мкА, 1 мкВ/м, 1 мкА/м, 1 мВт/м2.

Анализатор спектра должен быть программируемым, для дистанционного управления, т. е. должен обрабатывать команды, которые ему посылает ПЭВМ.

Должен иметь интерфейсы LAN или USB, или GPIB, или RS-232 для передачи данных с ПЭВМ на анализатор спектра и обратно.

Анализатор спектра должен иметь квазипиковый, пиковый и со среднеквадратичным отклонением детекторы.

Работать в полосе частот 9 кГц...1000 МГц.

Иметь полосы пропускания в диапазоне 1 кГц...3 МГц. Погрешность, вносимая собственными шумами, должна быть не более 1 дБ. Анализатор спектра должен обеспечивать звуковой контроль ПЭМИ, имеющих амплитудную и частотную (на частотах свыше 30 МГц) модуляцию, с помощью встроенных или подключаемых приборов или устройств.

Примерный перечень оборудования приведен в (табл. 1).

Таблица 1. Перечень оборудования для проведения оценки защищенности по каналу ПЭМИН

Наименование средств измерения	Тип	Диапазон частот
Анализатор спектра	LIGNext1 NS-30A	10 кГц -3 ГГц
Антенна магнитная рамочная активная	H-30	10 Гц – 30 МГц
Антенна электрическая дипольная активная	E-3000	30 МГц – 3000 МГц
Антенна электрическая дипольная	E-30	10 Гц – 30 МГц

активная		
Пробник напряжения	П-400	10 Гц – 300 МГц
Осциллограф	LeCroy Wavesurfer 62Xs	0 Гц – 600 МГц
Генератор сигналов	Г4-218	200 кГц-1 ГГц

Альтернативная измерительная площадка.

Временная методика оценки защищенности ОТСС, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации (КИ), описанная в «Сборнике временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам» предполагает собой поиск и измерение опасных сигналов непосредственно на объекте информатизации.

Однако, шумовая обстановка на объекте информатизации весьма нестабильна. Помимо нестабильности она абсолютно неисследованная. Оператор при проведении измерений может столкнуться с таким явлением как «стоячая волна».

Стоячая волна (электромагнитная) – периодическое изменение амплитуды напряженности электрического и магнитного полей вдоль направления распространения, вызванное интерференцией, падающей и отраженной волн. Например, стоячая волна возникает при отражении волны от преград и неоднородностей в результате взаимодействия (интерференции), падающей и отражённой волн.

Присутствие такой волны во время проведения измерений однозначно приведёт к ошибке.

Измерительная площадка – площадка, отвечающая требованиям, обеспечивающим правильное измерение уровней индустриальных радиопомех (ИРП), излучаемых ТС в регламентированных условиях. Видов ИП предусматриваются два – «открытая измерительная площадка» и «альтернативная

измерительная площадка». Поскольку строительство и эксплуатация открытой площадки весьма дорого, сосредоточимся на более дешёвом варианте – АИП. Разница между открытой ИП и АИП заключается в том, что последняя должна размещаться не в открытом пространстве, а в некотором помещении, в здании. При том физические характеристики АИП (прежде всего «затухание» электромагнитного поля) должны оставаться в пределах установленного допуска.

Важно! Перед вводом в эксплуатацию АИП оценивается минимум искажений, вносимых в распределение электромагнитного поля ограждающими конструкциями помещения, который можно допустить. Иными словами, оператор заранее знает о наличии и характере «стоячих волн» и о характеристиках закона затухания электромагнитного поля. Это позволяет получать информацию об «опасных» информативных сигналах корректнее, чем на ОИ, на котором абсолютно не исследована шумовая обстановка.

Практическая часть.

Вопросы для самопроверки:

6) Назовите весь перечень оборудования для проведения оценки защищенности по ПЭМИ.
7) Дайте определение измерительной площадки в рамках данного задания.
8) Сколько существует видов измерительных площадок (ИП) и в чем их различие?
9) На сколько метров минимально и максимально предполагается плавное размещение антенны по высоте?
10) Какой должен быть коэффициент калибровки у антенн?

Практические задания:

3) Как по Вашему мнению вы представляете себе открытую измерительную площадку и альтернативную? Опишите их. В чем их основное различие? Ответ обоснуйте.
4) Представьте, что Вы начинающий сотрудник предприятия ООО «НПП «ИБЦ». Начался ваш седьмой рабочий день. Вы в обычном распорядке, получив задание, идете включать лабораторное автоматизированное рабочее место и ПАК. Неожиданным образом узнаёте, что откалиброванная антенна начала давать сбой. Вы (без особой паники) начинаете искать пути решения. По Вашему мнению, каковы основные три шага на пути решения этой проблемы? Ответ обоснуйте.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Теоретические основы компьютерной безопасности» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком образовательного процесса	тестирование	УК-1 ПК-3	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	УК-1 ПК-3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%***
Проводится в сроки, установ-	Экзамен	УК-1 ПК-3	2 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отве-	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: 1. знание основных понятий предмета; 2. умение использовать и

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
ленные графиком образовательного процесса				денное на процедуру – 20 минут на каждого студента		применять полученные знания на практике; 3. работа на практических занятиях; 4. знание основных научных теорий, изучаемых предметов; 5. ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
						занятиях; • не отвечает на вопросы

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.

Типовые вопросы, выносимые на экзамен (тестирование)

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

- Функции КСЗИ:
  создание механизмов защиты, сводящие до минимума возможность воздействия дестабилизирующих факторов на защищаемую информацию; непрерывное и оптимальное управление механизмами комплексной защиты
  обеспечение конфиденциальности, целостности, доступности информации
  обеспечение криптографической, программной и аппаратной защиты информации
  обеспечение защиты людей, материальных носителей, автоматизированных систем

- Требование безопасности повторного использования объектов противоречит:
  инкапсуляции
  наследованию
  полиморфизму

- Уровни модели OSI, по возрастанию:
  физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной
  сетевой, канальный, транспортный, сеансовый, прикладной, представления, физический
  прикладной, представления, физический, канальный, сетевой, транспортный, сеансовый
  физический, сетевой, канальный, транспортный, сеансовый, представления, прикладной

- Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на игровую программу могут быть наложены следующие ограничения:
  запрет на чтение каких-либо файлов, кроме конфигурационных
  запрет на изменение каких-либо файлов, кроме конфигурационных +
  запрет на установление сетевых соединений

- Уровни модели TCP/IP, по возрастанию:
  канальный, сетевой, транспортный, прикладной
  транспортный, канальный, сетевой, прикладной
  канальный, транспортный, сетевой, прикладной
  прикладной, сетевой, транспортный, канальный

- К какому уровню модели TCP\IP относятся следующие протоколы HTTP, RTP, FTP, DNS:
  прикладной
  транспортный
  сетевой
  канальный

- В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
  меры обеспечения целостности
  административные меры
  меры административного воздействия

- Что входит в функции систем мониторинга:
  выявление состояния систем
  установка отношений между объектами
  установка соответствия правил и обязанностей
  все варианты верны

- Какие существуют подходы по построению защищенных операционных систем применяемых в АС:
  фрагментарный и комплексный
  фрагментарный и операционный.
  комплексный и позиционный.
  системный и позиционный.

- Дублирование сообщений является угрозой:
  доступности
  конфиденциальности
  целостности

- Какие существуют методы оценки качества КСИБ:
  метод оценки уязвимости Хоффмана +
  экспертная оценка +
  сигнатурный метод

качественный метод.

- Самыми опасными источниками внутренних угроз являются:
  некомпетентные руководители
  обиженные сотрудники
  любопытные администраторы

- Для внедрения бомб чаще всего используются ошибки типа:
  отсутствие проверок кодов возврата
  переполнение буфера
  нарушение целостности транзакций

- В число целей политики безопасности верхнего уровня входят:
  решение сформировать или пересмотреть комплексную программу безопасности
  обеспечение базы для соблюдения законов и правил
  обеспечение конфиденциальности почтовых сообщений

- В число целей программы безопасности верхнего уровня входят:
  управление рисками
  определение ответственных за информационные сервисы
  определение мер наказания за нарушения политики безопасности

- Что означает обеспечение целостности баз данных.

  это соответствие информации базы данных её внутренней логике, структуре и заданным правилам. +
  это полное значение информации базы данных в котором действуют установленные правила
  это информация, работающая по установленной структуре базы данных.
  это логическая операция обеспечивающая полноту информации и соблюдающая условия того, что информация не будет изменена.

- В рамках программы безопасности нижнего уровня осуществляются:
  стратегическое планирование
  повседневное администрирование
  отслеживание слабых мест защиты +

- Политика безопасности строится на основе:
  общих представлений об ИС организации
  изучения политик родственных организаций
  анализа рисков

- В число целей политики безопасности верхнего уровня входят:
  формулировка административных решений по важнейшим аспектам реализации программы безопасности

выбор методов аутентификации пользователей
обеспечение базы для соблюдения законов и правил +

- Основные механизмы защиты применяемые в ОС:
  идентификации / аутентификации
  разграничения доступа
  аудита
  все перечисленные варианты верны

4.2.Типовые вопросы, выносимые на экзамен

1. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности.
2. Структура информационных ресурсов и администрирование в компьютерных системах.
3. Проблемы безопасности компьютерных систем (сетей), понятие угрозы, цели злоумышленников, осуществляющих основные атаки.
4. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников
5. Уязвимости автоматизированных систем (АС), возможные атаки на них. Особенности построения систем обнаружения атак (СОА) в АС.
6. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.
7. Факторы, воздействующие на защищаемую информацию. Классификация угроз. Естественные и искусственные угрозы. Основные направления и методы реализации угроз.
8. Основные виды атак на КС, их классификация. Проблемы обеспечения информационной безопасности в проводных КС.
9. Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.
10. Основные уровни защиты информации в компьютерных системах, организация системы безопасности по уровням компьютерных систем, уровни защиты, в соответствии с механизмами реагирования на угрозы.
11. Машинные носители информации (МНИ), защита МНИ, защита средств взаимодействия с МНИ.
12. Методы и средства обеспечения защиты информации в компьютерных системах, защита представления информации, защита содержания информации.
13. Представьте обобщенную модель защиты объекта, содержащего локальную вычислительную сеть, с безопасной обработкой информации.

14. Какие стадии включает жизненный цикл системы защиты информации (СЗИ), если СЗИ рассматривать как сложную техническую систему? Охарактеризуйте какие процессы включает каждая из стадий.
15. Какие объекты информатизации, инженерные, технические и программно-аппаратные способы и средства могут быть использованы для защиты информации в коммерческих структурах?
16. Перечислите рекомендуемые СТР-К стадии создания системы защиты информации (СЗИ). Какие вопросы решаются на предпроектной стадии, кем она выполняется и чем заканчивается.
17. Сертификация программных и программно-технических средств защиты конфиденциальной компьютерной информации.
18. Методы обеспечения защиты информации – препятствие, маскировка, управление доступом. Функции защиты при управлении доступом. Принуждение и побуждение.
19. Физические средства защиты компьютерных систем. Нейтрализация утечки информации по электромагнитным каналам – применение генераторов шума. Защита от наводок.
20. Аксиомы и определения доступа субъектов к объектам. Понятие объекта относительно языка L. Объекты, входящие в состав компьютерных систем.
21. Аксиома доступа субъектов к объектам. Определение понятия разграничения доступа. Методы разграничения доступа.
22. Дискреционное разграничение доступа. Матрицы доступа. Списки полномочий.
23. Полномочное (мандатное) разграничение доступа. Разграничение по уровням секретности. Различие между дискреционным и мандатным разграничением доступа.
24. Концепция монитора безопасности обращений в компьютерную систему. Правила разграничения доступа субъектов к объектам в ОС.
25. Монитор безопасности обращений (МБО) субъектов к объектам. Схема монитора безопасности обращений. Функции МБО. Свойства МБО.
26. Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана.
27. Формальное описание системы в модели Харрисона-Руззо-Ульмана. Поведение системы во времени. Понятие монооперационной системы.
28. Теорема о существовании алгоритма определения исходного состояния системы. Условие использования классической модели Харрисона-Руззо-Ульмана. Разрешимость проблемы безопасности.

29. Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.
30. Граф доступов. Правила определения переходов системы из состояния в состояние. Условия реализации прав доступа. Расширенная модель Take-Grant, анализ информационных каналов.
31. Пути и стоимости возникновения информационных потоков в расширенной модели Take-Grant.
32. Общий подход к построению систем, реализующих мандатную (полномочную) политику безопасности в модели BL (Белла-Лападулы).
33. Назначение модели Белла-Лападулы. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы.
34. Условие определения безопасности системы. Свойства безопасности системы. Проверка безопасности системы. Основные теоремы и определения состояний системы.
35. Эквивалентные подходы к определению безопасности модели Белла-Лападулы. Недостатки модели Белла-Лападулы.
36. Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA.
37. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.
38. Требования, предъявляемые к формированию политики безопасности организации. Структура и содержание политики безопасности организации применительно к компьютерным системам.
39. Реализация политики безопасности в компьютерных системах (КС) с использованием механизмов и средств операционных систем. Управление доступом в КС с использованием механизмов и средств сетевых операционных систем.
40. Управление инцидентами информационной безопасности в компьютерных системах.
41. Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации.
42. Фрагментарный и комплексный подходы к созданию систем защиты. Основные достоинства и недостатки фрагментарного подхода. Организация защищенной среды обработки информации при комплексном подходе. Недостатки комплексного подхода.
43. Построение систем защиты от угрозы нарушения конфиденциальности информации. Модель системы защиты от угроз нарушения конфиденциаль-

ности информации. Структура системы защиты от угроз нарушения конфиденциальности информации.

44. Построение систем защиты от угрозы нарушения целостности информации. Две основные группы организационно-технологических мер защиты целостности информации. Технологические меры контроля целостности битовых последовательностей, хранящихся на машинных носителях.

45. Построение системы защиты от угрозы нарушения доступности информации. Понятие доступности информации. Основные угрозы доступности информации. Причины возникновения угроз доступности информации. Основные средства защиты от угрозы нарушения доступности информации.

47. Особенности построения парольных систем аутентификации. Парольная защита. Понятия идентификатора и пароля пользователя. Учетная запись пользователя как совокупность его идентификатора и его пароля. Парольная система и состав её элементов.

48. Основные угрозы безопасности парольных систем. Способы получения пароля злоумышленником. Рекомендации по практической реализации парольных систем. Оценка стойкости парольных систем. Методы хранения и передачи паролей. Механизмы хранения паролей в КС.

49. Проблема организации совместного доступа различных приложений к некоторым областям памяти. Основные способы защиты памяти. Барьерные адреса. Механизм функционирования барьерного способа защиты памяти. Способы задания барьерного адреса. Динамические области памяти. Защита данных приложений.

50. Адресные регистры. Особенности способов защиты памяти. Ключ доступа. Организация совместного использования областей памяти. Механизм страничной организации памяти и сегментации.

51. Цифровая подпись. Проблема аутентификации данных или цифровой подписи. Модель аутентификации сообщений. Сравнительный анализ обычной и цифровой подписи.

52. Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи. Методы построения защищённых АС.

53. Что означает термин «аттестация объекта информатизации», раскройте это понятие, какие процедуры предусматриваются для аттестации автоматизированной системы?

54. Этапы разработки защищённой АС. Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2014). Цель создания автоматизированных систем в защищенном исполнении.

55. Понятие стандарта в области информационной безопасности (ИБ). Обоснование необходимости использования стандартов в области ИБ. Главная задача стандартов в области ИБ.
56. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.

57. Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.

Примерная тематика (контрольных заданий) задач для выполнения:

ЗАДАНИЕ № 1

Тема: Теоретические аспекты проведения специальных исследований (СИ) на предприятии

Цель работы.

Изучение основных принципов проведения специальных исследований на предприятии. Освоить структуру ведения общей теоретической части проведения специальных исследований.

Продолжительность занятия: полтора учебных часа.

Задания.

13. Изучить теоретическую часть Задания №1.
14. Выполнить практическую часть Задания №1:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

15. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Специальные исследования (специсследования, СИ) — комплекс действий, направленный на обнаружение потенциальных технических каналов

утечки защищаемой информации с помощью специального контрольно-измерительного оборудования, в соответствии с нормативно-методическими документами ФСБ России и ФСТЭК России.

Проведение специсследований определяет возможность считывания и перехвата сигнала специальными средствами разведки в рамках определённых границ (защищённость утечек по каналам ПЭМИН — побочные электромагнитные излучения и наводки).

Введем для большей ясности определения, связанные с основой ведения специсследований на предприятии. Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается ценная информация.

Автоматизированная система (АС) – устройство или комплекс устройств, необходимых для передачи, хранения и обработки конфиденциальной информации, прошедшая процедуру аттестации в соответствии с законодательством РФ.

Контролируемая зона (КЗ) – пространство, в котором исключено неконтролируемое пребывание посторонних лиц или сотрудников, не имеющих прямое отношение к данному пространству. Примерами могут послужить: периметр охраняемой территории; ограждающие конструкции охраняемого здания или охраняемой территории.

Информационный сигнал – электрические сигналы, акустические, электромагнитные и т.д., по параметрам которых можно раскрыть конфиденциальную информацию, передаваемую, хранимую или обрабатываемую в основных технических средствах и системах или обсуждаемая в защищенном исполнении.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для обработки, хранения и передачи конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

Средства активной защиты информации по каналам ПЭМИН (САЗ) – технические средства формирования маскирующих электромагнитных помех в местах возможного съема защищаемой информации, прошедшие обязательную процедуру сертификации по линии ФСТЭК России.

Деятельность по технической защите конфиденциальной информации (ТЗКИ) – выполнение работ и (или) оказание услуг по ее защите:

– от несанкционированного доступа,

– от утечки по техническим каналам,

– от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Важно! Данный вид деятельности является лицензируемым. Лицензирование деятельности по ТЗКИ осуществляет ФСТЭК России.

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные поля, создаваемые в окружающем пространстве СВТ, специально для этого не предназначенными (в случае ПЭМИ) или наводки данных излучений на токоведущие конструкции, линии и подключенные к ним ТС.

Существует несколько видов проведения специсследований на определенные ТС. В данном случае это акустоэлектрическое преобразование (АЭП) и ПЭМИН. В случае АЭП исследуемое средство подвергается воздействию некоих акустических частот. Из этого обосновывается определенный вывод о возможности использования ТС на невозможности подверженности АЭП.

Как уже было указано в определениях, ПЭМИ создаются вокруг работающих технических средств, которые специально для данного излучения не создавались. То есть излучение от радиопередатчиков, мобильных телефонов

– это не побочные излучения. А вот излучения при работе компьютера от монитора, принтера, накопителей информации являются побочными.

Если вспомнить физику, то вокруг проводника, по которому протекает электрический ток возникает электромагнитное поле. Если по данному проводнику передается какой-либо сигнал, то, следовательно, и электромагнитное поле тоже будет изменяться по тем же законам, что и сигнал, протекающий в линии. Таким образом, источником сигнала ПЭМИ являются все токоведущие линии в ТС, по которым в процессе работы передаются какие-либо сигналы.

Как известно электромагнитные поля могут распространяться на значительные расстояния и конструкции помещений тому не преграда. Скорость передачи данных и обработки информации в современных средствах вычислительной техники постоянно растет, а значит растут и частоты сигналов ПЭМИ. Частоты сигналов ПЭМИ могут начинаться от единиц кГц и заканчиваться единицами ГГц, а гармоники этих сигналов могут находиться еще выше по частоте.

Если вспомнить, что в проводнике, помещенном в электромагнитное поле, возникает электрический ток, то очевидно, что могут возникать наводки ПЭМИ на любые токоведущие элементы (систему отопления, короб системы вентиляции и т. д.), в том числе и любые линии и ТС, подключенные к ним, попадающие под действие данного электромагнитного поля.

Перехват этой информации можно осуществить путем анализа изменений параметров ПЭМИН с помощью специальных высокочувствительных радиоприемных устройств, оснащенных специализированными антеннами, пробниками напряжения, токосъемниками.

На (рис. 1) приведена физика утечки информации за счет ПЭМИ.

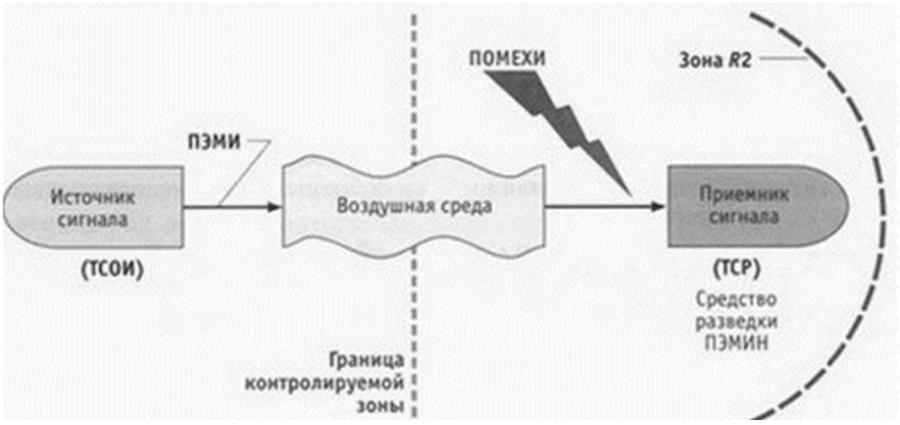


Рисунок 1. Схема ТКУИ за счет ПЭМИ

На (рис. 2) приведена физика утечки информации за счет ПЭМИН.

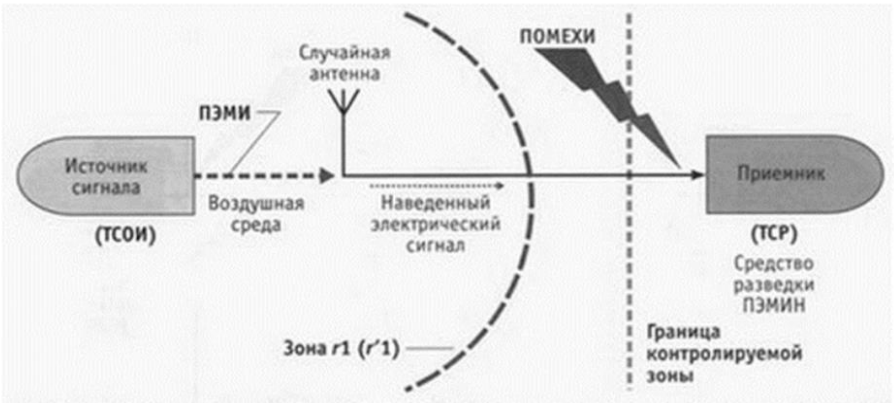


Рисунок 2. Схема ТКУИ за счет ПЭМИН

Поясним некоторые сокращения и термины на схемах:

- ТСОИ – технические средства обработки информации (все что попадает под определение ОТСС);
- ТСР–технические средства разведки;
- зона R2 – расстояние, на котором возможен перехват защищаемой информации за счет ПЭМИ;
- зона r1(r'1) – расстояние, наличие в пределах которого случайных антенн (токоведущие конструкции, линии и ТС) создает возможность утечки информации за счет наводок ПЭМИ.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенной случайной антенной может являться стационарный телефон, датчик пожарной сигнализации, громкоговоритель, подключенная к линии, выходящей за пределы КЗ.

Распределенные случайные антенным – антенны с распределенными параметрами. К ним можно отнести: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ.

Также разделяют саму информации по каналам АЭП и ПЭМИ на случай информативности. Информативные – сигналы с несущей, модулированной информативным сигналом. Примером могут послужить: сигнал от флэш-накопителя USB; VGA-интерфейс монитора; и т.д.

Неинформативные сигналы – сигналы, анализ которых не дает представления об обрабатываемой информации. Примеры: излучения от работы источников питания в узлах ТС; сигнал обработки режимов видеокартой; и т.д.

Важно! Всё приведенное выше относится к составной части по проведению работ, связанных с специальными исследованиями ОТСС и ВТСС. Однако это лишь малая часть того, что можно было бы изложить. Остальная теоретическая и прикладная часть изучается непосредственно работником предприятия в режимно секретном подразделении. Все методические материалы работ, связанных с проведением специальных исследований имеют грифы СЕКРЕТНО и СОВЕРШЕННО СЕКРЕТНО. Вышеизложенный материал является открытым и считается опорным в общих знаниях ТЗИ.

Практическая часть.

Вопросы для самопроверки:

11) Дайте определение специальным исследованиям в рамках данного учебного занятия.
12) Какие и сколько существует грифов секретности в рамках законодательства РФ?
13) Что такое зона r1(r’1) в ТЗИ?
14) Дайте определение ОТСС и ВТСС и в чем их различие?

15) На какие категории разбиваются случайные антенны в КЗ и в чем их разница? И на какие категории разбиваются информационные сигналы и в чем их разница?

Практические задания:

5) Опишите собственными словами следующие определения. ОТСС; ВТСС; ТКУИ.
6) В соответствии с (рис. 1) данного учебного задания, источником распространения сигнала ПЭМИ между техническим средством и техническим средством разведки является воздушная среда. Что будет если изменить воздушную среду на более плотную, а что, если перенести её в вакуум. Ответ обоснуйте.

Однажды, двое ученых задались очень интересной задачей, связанной с передачей информативного сигнала технического средства через канал ПЭМИ по очень интересной схеме. У них получилось и даже на современном этапе злоумышленники охотно придают значение данному средству получения заведомо важной для них информации. Двух ученых звали Маркус Кун и Росс Андерсон. При помощи сети Интернет, найдите информацию о данной процедуре получения информативного сигнала по каналу ПЭМИ и расскажите в общих чертах об этой технологии

ЗАДАНИЕ № 2

Тема: Теоретические основы средств измерения программно-аппаратных комплексов (ПАК) и альтернативной измерительной площадки (АИП)

Цель работы.

Изучение теоретической основы средств измерений сигналов. Освоить особенности поиска и идентификации сигналов при помощи альтернативной измерительной площадки.

Продолжительность занятия: полтора учебных часа.

Задания.

16. Изучить теоретическую часть Задания №2.
17. Выполнить практическую часть Задания №2:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

18. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

В связи с тем, что многие организации, занимающиеся производством и распространением программно-аппаратных комплексов, предлагают на рынке целые линейки своих продуктов, отличающихся только аппаратной частью (анализаторы спектра) и соответственно ценой на данные товары в этой линейке. На рынке представлены программ- но-аппаратные комплексы следующих производителей, распространителей: «Навигатор ПхГ» – «НЕЛК», «Сигурд Мх» – «МАСКОМ», «Легенда» – «АВМ-СИСТЕМС». Стоит отметить, что все комплексы, рассматриваемые в данной работе, имеют сертификаты ФСТЭК России и метрологический сертификат соответствия на измерительное оборудование. Пример ПАК представлен на (рис. 1).

Рисунок 1. ПАК «Сигурд М18»

Требования к антеннам.

В полосе частот от 200 Гц до 30 МГц в комплект антенн должны входить магнитная и (или) электрическая антенны.

Для измерения магнитной составляющей электромагнитного поля, антенна должна быть: электрически экранированной рамочной антенной, имеющей такие размеры, чтобы ее рамка помещалась в квадрат со стороной не более 0,6 м, или ферритовая антенна длиной не более 0,5 м.

Допускаемая погрешность измерений напряженности магнитного поля (измеритель с магнитной антенной) не должна превышать 2,5 дБ.

Конструкция антенн (антенного штатива) должна обеспечивать возможность плавного изменения высоты расположения антенны над землей от 0,8 м до 1,25 м, а также возможность поворота магнитной и электрической антенн на 360° вокруг оси.

В полосе частот от 30 до 1000 МГц в комплект антенн должны входить одна или несколько электрических антенн одного из следующих типов:

а) линейный симметричный вибратор на полосу частот от 30 до 80 МГц, размер которого равен длине полуволнового симметричного вибратора на частоте 80 МГц, и настраиваемый полуволновой симметричный вибратор в полосе частот от 80 до 1000 МГц, имеющий КСВН не более 2,5;

б) биконическая антенна, максимальный размер которой должен быть не более 1,35 м в полосе частот от 30 до 300 МГц и с КСВН не более 3,0, и биконическая антенна, максимальный размер которой – не более 0,5 м в полосе частот от 300 до 1000 МГц с КСВН не более 2,5;

в) широкополосная антенна, главный лепесток диаграммы направленности которой должен быть таким, чтобы в направлении непосредственного излучения от источника ПЭМИН и в направлении отраженного от земли луча разность коэффициентов усиления антенны не превышала бы 1 дБ, с КСВН не более 2,5.

Конструкция антенны (антенного штатива) должна обеспечивать возможность плавного изменения высоты центра симметрии над землей от 1 до

4 м и поворота вокруг горизонтальной оси на 180°, а также фиксированную ориентацию в трех взаимно ортогональных направлениях.

Допускаемая погрешность измерений напряженности электрического поля (измеритель с биконической, электрической антенной) не должна превышать 2,5 дБ на частотах до 1000 МГц.

Антенны должны иметь коэффициент калибровки, позволяющий измерять уровни полей. Рекомендуемый коэффициент калибровки антенн – не более 40 дБ. Погрешность коэффициента калибровки антенн должна быть не более 2 дБ.

Требования к анализатору.

Должен иметь несимметричный вход с номинальным значением сопротивления 50 Ом с коэффициентом стоячей волны по напряжению (КСВН) не более 2 при ослаблении входного аттенюатора 0 дБ и не более 1,2 при ослаблении входного аттенюатора 10 дБ и более.

Измерители совместно с первичными преобразователями должны обеспечивать измерения характеристик ПЭМИ в децибелах, относительно 1 мкВ, 1 мкА, 1 мкВ/м, 1 мкА/м, 1 мВт/м2.

Анализатор спектра должен быть программируемым, для дистанционного управления, т. е. должен обрабатывать команды, которые ему посылает ПЭВМ.

Должен иметь интерфейсы LAN или USB, или GPIB, или RS-232 для передачи данных с ПЭВМ на анализатор спектра и обратно.

Анализатор спектра должен иметь квазипиковый, пиковый и со среднеквадратичным отклонением детекторы.

Работать в полосе частот 9 кГц...1000 МГц.

Иметь полосы пропускания в диапазоне 1 кГц...3 МГц. Погрешность, вносимая собственными шумами, должна быть не более 1 дБ. Анализатор спектра должен обеспечивать звуковой контроль ПЭМИ, имеющих амплитудную и частотную (на частотах свыше 30 МГц) модуляцию, с помощью встроенных или подключаемых приборов или устройств.

Примерный перечень оборудования приведен в (табл. 1).

Таблица 1. Перечень оборудования для проведения оценки защищенности по каналу ПЭМИН

Наименование средств измерения	Тип	Диапазон частот
Анализатор спектра	LIGNext1 NS-30A	10 кГц -3 ГГц
Антенна магнитная рамочная активная	Н-30	10 Гц – 30 МГц
Антенна электрическая дипольная активная	Е-3000	30 МГц – 3000 МГц
Антенна электрическая дипольная активная	Е-30	10 Гц – 30 МГц
Пробник напряжения	П-400	10 Гц – 300 МГц
Осциллограф	LeCroy Wavesurfer 62Xs	0 Гц – 600 МГц
Генератор сигналов	Г4-218	200 кГц-1 ГГц

Альтернативная измерительная площадка.

Временная методика оценки защищенности ОТСС, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации (КИ), описанная в «Сборнике временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам» предполагает собой поиск и измерение опасных сигналов непосредственно на объекте информатизации.

Однако, шумовая обстановка на объекте информатизации весьма нестабильна. Помимо нестабильности она абсолютно неисследованная. Оператор при проведении измерений может столкнуться с таким явлением как «стоячая волна».

Стоячая волна (электромагнитная) – периодическое изменение амплитуды напряженности электрического и магнитного полей вдоль направления

распространения, вызванное интерференцией, падающей и отраженной волн. Например, стоячая волна возникает при отражении волны от преград и неоднородностей в результате взаимодействия (интерференции), падающей и отражённой волн.

Присутствие такой волны во время проведения измерений однозначно приведёт к ошибке.

Измерительная площадка – площадка, отвечающая требованиям, обеспечивающим правильное измерение уровней индустриальных радиопомех (ИРП), излучаемых ТС в регламентированных условиях. Видов ИП предусматриваются два – «открытая измерительная площадка» и «альтернативная измерительная площадка». Поскольку строительство и эксплуатация открытой площадки весьма дорого, сосредоточимся на более дешёвом варианте – АИП. Разница между открытой ИП и АИП заключается в том, что последняя должна размещаться не в открытом пространстве, а в некотором помещении, в здании. При том физические характеристики АИП (прежде всего «затухание» электромагнитного поля) должны оставаться в пределах установленного допуска.

Важно! Перед вводом в эксплуатацию АИП оценивается минимум искажений, вносимых в распределение электромагнитного поля ограждающими конструкциями помещения, который можно допустить. Иными словами, оператор заранее знает о наличии и характере «стоячих волн» и о характеристиках закона затухания электромагнитного поля. Это позволяет получать информацию об «опасных» информативных сигналах корректнее, чем на ОИ, на котором абсолютно не исследована шумовая обстановка.

Практическая часть.

Вопросы для самопроверки:

11) Назовите весь перечень оборудования для проведения оценки защищенности по ПЭМИ.

12) Дайте определение измерительной площадки в рамках данного задания.
13) Сколько существует видов измерительных площадок (ИП) и в чем их различие?
14) На сколько метров минимально и максимально предполагается плавное размещение антенны по высоте?
15) Какой должен быть коэффициент калибровки у антенн?

Практические задания:

5) Как по Вашему мнению вы представляете себе открытую измерительную площадку и альтернативную? Опишите их. В чем их основное различие? Ответ обоснуйте.
6) Представьте, что Вы начинающий сотрудник предприятия ООО «НПП «ИБЦ». Начался ваш седьмой рабочий день. Вы в обычном распорядке, получив задание, идете включать лабораторное автоматизированное рабочее место и ПАК. Неожиданным образом узнаёте, что откалиброванная антенна начала давать сбой. Вы (без особой паники) начинаете искать пути решения. По Вашему мнению, каковы основные три шага на пути решения этой проблемы? Ответ обоснуйте.

Приложение 2

Методические указания для обучающихся по освоению дисциплины (модуля)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль): Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Общие положения

Цель дисциплины:

Целью изучения дисциплины является формирование у обучаемых концептуальных и методологических основ в области теории обеспечения информационной безопасности в процессе развития современного информационного общества на всех уровнях функционирования Российской Федерации: межгосударственном, государственном, ведомственном и отдельных граждан.

Задачи дисциплины:

- раскрытие сущности, целей и содержание основ теории информационной безопасности и методологии защиты информации в автоматизированных телекоммуникационных системах;
- ознакомление студентов с теоретическими основами и нормативной базой, применяемых для построения защищенных информационных систем;
- формирование у студентов базовых знаний в области технологий и механизмов защиты информации, применяемых в компьютерных системах;
- привитие студентам навыков практической работы с программно-аппаратными средствами защиты информации;
- подготовка студентов применять стандарты по оценке информационной защищённости при анализе и проектировании защищённых компьютерных систем.

2. Указания по проведению практических (семинарских) занятий

Тема 1. Введение. Основные понятия теории компьютерной безопасности

Практическое занятие 1

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: групповая дискуссия

Тема и содержание практического занятия: Актуальность проблемы обеспечения информационной безопасности (ИБ) в компьютерных системах. Современная постановка целей и задач по обеспечению компьютерной безопасности (переход к тотальной защите и интенсивным мерам). Основные термины и определения в области ИБ компьютерных систем и сетей.

Цель работы: Получить практические знания и навыки о классификации компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и по функциональному назначению, а также знания о проблематике обеспечения компьютерной безопасности.

Учебные вопросы:

- Современная постановка целей и задач по обеспечению компьютерной безопасности (переход к тотальной защите и интенсивным мерам).

• Основные термины и определения в области ИБ компьютерных систем и сетей.

• Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения.

• Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности.

• Факты, свидетельствующие о способах злоупотребления информацией, циркулирующей в компьютерных системах.

• Продолжительность практического занятия-1 часа

Тема 2. Анализ угроз информационной безопасности для компьютерных систем

Практическое занятие 2

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: подготовка реферата

Тема и содержание практического занятия: Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников. Уязвимости АС, возможные атаки на них. Особенности построения систем обнаружения атак (СОА) в АС. Фундаментальные угрозы – утечка информации, нарушение целостности, отказ в обслуживании, незаконное использование. Первичные угрозы – проникновение (маскарад, обход защиты, нарушение полномочий) и внедрение (троянские программы, потайные ходы).

Цель работы: Получить практические знания и навыки об угрозах и возможных атаках, которым могут быть подвергнуты информационные системы.

Учебные вопросы:

• Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.

• Уязвимости АС, возможные атаки на них.

• Особенности построения систем обнаружения атак (СОА) в АС.

• Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.

• Причины возникновения угроз безопасности информации. Отличительные особенности угроз корпоративным и локально-вычислительным сетям.

• Продолжительность практического занятия-1 часа

Тема 3. Основные уровни защиты информации в компьютерных системах

Практическое занятие 3

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: групповая дискуссия

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки об уровнях защиты информации в компьютерных системах.

Учебные вопросы:

- Организация системы безопасности по уровням компьютерных систем (КС). Уровни защиты, в соответствии с механизмами реагирования на угрозы.
- Способы защиты данных на различных уровнях. Организация системы безопасности по уровням.
- Машинные носители информации (МНИ). Защита МНИ. Защита средств взаимодействия с МНИ.
- Основные особенности компьютерной информации с точки зрения доступа к ней злоумышленников.
- Виды защищаемой компьютерной информации.
- Условия доступа к защищаемой информации со стороны злоумышленников.
- Продолжительность практического занятия-1 часа

Тема 4. Основные положения формальной теории защиты информации

Практическое занятие 4

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: практическая работа в группах

Тема и содержание практического занятия: Аксиомы и определения доступа субъектов к объектам. Понятие объекта относительно языка L. Объекты, входящие в состав КС. Язык описания клавиатуры. Преобразование. Пример преобразования. Инициирование действия преобразования. Два состояния преобразования. Понятие домена. Процесс. Определение субъекта. Виды доступа к субъекту. Информационный поток. Запись.

Цель работы: Получить практические знания и навыки по методам разграничения доступа в информационных системах.

Учебные вопросы:

- Аксиома доступа субъектов к объектам.
- Определение понятия разграничения доступа. Методы разграничения доступа.

• Дискреционное разграничение доступа. Матрицы доступа. Списки полномочий.

• Полномочное (мандатное) разграничение доступа. Разграничение по уровням секретности.

• Различие между дискреционным и мандатным разграничением доступа.

• Ролевое разграничение доступа.

Продолжительность практического занятия-1 часа

Тема № 5. Формальные модели безопасности

Практическое занятие 5

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: групповая дискуссия

Тема и содержание практического занятия: Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU).

Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.

Цель работы: получить практические знания и навыки об основных формальных логических моделях доступа.

Учебные вопросы:

• Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU).

• Моделирование поведения системы во времени. Основные команды и операции, моделирующие поведение системы. Примеры команд, используемых при переходе системы из одного состояния в другое.

• Формальное описание системы в модели HRU. Поведение системы во времени.

• Понятие монооперационной системы. Теорема о существовании алгоритма определения исходного состояния системы. Условие использования классической модели HRU. Разрешимость проблемы безопасности.

• Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant.

• Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.

• Граф доступов. Правила определения переходов системы из состояния в состояние. Условия реализации прав доступа.

• Расширенная модель Take-Grant, анализ информационных каналов.

- Пути и стоимости возникновения информационных потоков в расширенной модели Take-Grant.
- Продолжительность практического занятия-2 часа

Тема № 6. Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам

Практическое занятие 6

Вид практического занятия: смешанная форма практического занятия.

Образовательные технологии: практическая работа в группах

Тема и содержание практического занятия: Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.

Требования, предъявляемые к формированию политики безопасности организации. Структура и содержание политики безопасности организации применительно к компьютерным системам.

Цель работы: получить практические знания и навыки об управлении информационной безопасностью и формированию политики информационной безопасности в организации.

Учебные вопросы:

- Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA.
- Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.
- Требования, предъявляемые к формированию политики безопасности организации.
- Структура и содержание политики безопасности организации применительно к компьютерным системам.
- Цель работы: получить практические знания и навыки об управлении информационной безопасностью и формированию политики информационной безопасности в организации.
- Продолжительность практического занятия-2 часа

Тема № 7. Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации

Практическое занятие 7

Вид практического занятия: смешанная форма практического занятия.

Образовательные технологии: подготовка реферата

Тема и содержание практического занятия: Фрагментарный и комплексный подходы к созданию систем защиты. Основные достоинства и недостатки фрагментарного подхода. Организация защищенной среды обработки информации при комплексном подходе. Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации.

Цель работы: получить практические знания и навыки по построению систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации.

Учебные вопросы:

- Фрагментарный и комплексный подходы к созданию систем защиты. Основные достоинства и недостатки фрагментарного подхода.
- Организация защищенной среды обработки информации при комплексном подходе. Недостатки комплексного подхода. Условия эффективной работы средств защиты информации.
- Организация защиты субъектов информационных отношений.
- Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации.
- Построение систем защиты от угрозы нарушения конфиденциальности информации. Модель системы защиты от угроз нарушения конфиденциальности информации. Структура системы защиты от угроз нарушения конфиденциальности информации.
- Построение систем защиты от угрозы нарушения целостности информации. Две основные группы организационно-технологических мер защиты целостности информации.
- Технологические меры контроля целостности битовых последовательностей, хранящихся на машинных носителях.
- Циклический контрольный код как механизм обеспечения контроля целостности информации.
- Интегрированный подход для обеспечения целостности данных. Основные принципы обеспечения целостности данных. Обеспечение защиты целостности программно-аппаратной среды.
- Построение системы защиты от угрозы нарушения доступности информации. Понятие доступности информации.
- Основные угрозы доступности информации. Причины возникновения угроз доступности информации.
- Основные средства защиты от угрозы нарушения доступности информации.
- Продолжительность практического занятия-2 часа

Тема № 8. Методология обследования и проектирования защищенных информационных (автоматизированных) систем

Практическое занятие 8

Вид практического занятия: смешанная форма практического занятия.

Образовательные технологии: практическая работа в группах

Тема и содержание практического занятия: Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи. Методы построения защищённых АС. Принципы проектирования. Структурный принцип и принцип модульного проектирования. Три основных конструкции для проектирования. Преимущества использования модульного принципа.

Корректность реализации и верификация информационных (автоматизированных) систем. Понятие корректности или правильности проверяемого объекта. Спецификация требований программного обеспечения.

Представления функциональных требований. Рекомендации к структуре и методам описания программных требований. Основные ключевые требования «хорошей спецификации». Требования к программной спецификации. Основные подходы к определению спецификаций требований.

Теория безопасных систем (ТСВ). Понятие «доверенная вычислительная среда» (trusted computing base-TCB). Дискретная природа характеристики «безопасный». Характеристика «доверенный». Доверенная вычислительная среда. Набор компонентов, составляющий доверенную вычислительную среду. Этапы разработки защищённой АС. Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2000). Цель создания АСЗИ.

Цель работы: получить практические знания и навыки об этапах и содержании работ по проектированию защищенных информационных (автоматизированных) систем.

Учебные вопросы:

- Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи.
- Методы построения защищённых АС. Два основных метода проектирования. Метод проектирования «снизу вверх». Недостатки метода проектирования «снизу вверх».
- Иерархический метод построения защищённой АС («сверху вниз»).
- Принципы проектирования. Структурный принцип и принцип модульного проектирования.
- Три основных конструкции для проектирования. Использование элемента DO-WHILE для организации цикла. Конструкция принятия двоичного решения IF-THEN-ELSE. Преимущества использования модульного принципа.
- Корректность реализации и верификация информационных (автоматизированных) систем. Понятие корректности или правильности проверяемого объекта.

• Спецификация требований программного обеспечения. Функциональные критерии и характеристики. Неформализованные представления разработчика. Спецификация требований программного обеспечения (Software Requirements Specification).

• Представления функциональных требований. Рекомендации к структуре и методам описания программных требований. Основные ключевые требования «хорошей спецификации». Требования к программной спецификации. Основные подходы к определению спецификаций требований.

• Теория безопасных систем (ТСВ). Понятие «доверенная вычислительная среда» (trusted computing base-TCB).

• Дискретная природа характеристики «безопасный». Характеристика «доверенный». Доверенная вычислительная среда. Набор компонентов, составляющий доверенную вычислительную среду.

• Этапы разработки защищённой автоматизированной системы (АСЗИ). Процесс создания автоматизированных систем в защищенном исполнении (ГОСТ Р 51583—2014). Цель создания АСЗИ.

• Продолжительность практического занятия-2 часа

Тема № 9. Общие сведения о стандартах в области информационной безопасности
Практическое занятие 9

Вид практического занятия: смешанная форма практического занятия.

Образовательные технологии: практическая работа в группах

Тема и содержание практического занятия: Понятие стандарта в области информационной безопасности (ИБ). Обоснование необходимости использования стандартов в области ИБ. Главная задача стандартов в области ИБ. Стандарты как основной механизм обеспечения совместимости продуктов и систем.

Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.

Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.

Аудит. Идентификация и аутентификация. Механизм защиты данных. Регистрация и учёт. Корректность. Контроль корректности функционирования средств защиты. Непрерывность защиты.

Основные положения «Общих критериев». Свойство «Общих критериев». Структура «Общих критериев». Определение объекта оценки и продукта. Система как специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

Профили защиты. Введение профиля защиты. Идентификация профиля защиты. Аннотация профиля защиты. Описание объекта оценки. Характерные особенности ИТ применительно к объекту оценки (ОО).

Среда безопасности ОО. Описание аспектов безопасности среды, в которой предполагается использовать ОО. Структура и содержание профиля защиты. Цели безопасности для ОО. Цели безопасности для среды ОО.

Функциональные требования и требования доверия. Основные осуществляемые операции при выборе компонентов функциональных требований. Требования доверия к безопасности ОО. Обоснование профиля защиты.

Цель работы: получить практические знания и навыки о применении стандартов в области информационной безопасности

Учебные вопросы:

- Понятие стандарта в области информационной безопасности (ИБ). Обоснование необходимости использования стандартов в области ИБ. Главная задача стандартов в области ИБ. Стандарты как основной механизм обеспечения совместимости продуктов и систем.
- Основы взаимодействия между производителями, потребителями и экспертами по квалификации продуктов информационных технологий (ИТ). Регламентация необходимости применения средств, механизмов, алгоритмов. Требования безопасности.
- Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации.
- Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.
- Набор требований к подсистемам защиты АС. Проверка соответствия требованиям по защите информации от НСД для АС. Показатели защищённости от НСД к информации в АС.
- Стандарт «Критерии оценки доверенных компьютерных систем»/ TCSEC («Оранжевая книга»). Цель разработки стандарта TCSEC. Требования безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем. Категории требований безопасности. Общая структура требований к системам защиты.
- Политика безопасности. Возможность осуществления субъектами доступа к объектам. Разграничение доступа к категорированной информации. Метки безопасности как механизм контроля доступа.
- Аудит. Идентификация и аутентификация. Механизм защиты данных. Регистрация и учёт. Корректность. Контроль корректности функционирования средств защиты. Непрерывность защиты.
- Основные положения «Общих критериев». Свойство «Общих критериев». Структура «Общих критериев». Определение объекта оценки и продук-

та. Система как специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

- Категории пользователей. Среда безопасности. Задачи, решаемые при подготовке к оценке. Требования по безопасности. Каталоги требований безопасности. Общая модель безопасности. Недостатки «Общих критериев».
- Профили защиты. Введение профиля защиты. Идентификация профиля защиты. Аннотация профиля защиты. Описание объекта оценки. Характерные особенности ИТ применительно к объекту оценки (ОО).
- Среда безопасности ОО. Описание аспектов безопасности среды, в которой предполагается использовать ОО. Структура и содержание профиля защиты. Цели безопасности для ОО. Цели безопасности для среды ОО.
- Функциональные требования и требования доверия. Основные осуществляемые операции при выборе компонентов функциональных требований. Требования доверия к безопасности ОО. Обоснование профиля защиты.
- Продолжительность практического занятия-2 часа

Тема № 10. Концепция защиты СВТ и АС от НСД в соответствии с руководящими документами Гостехкомиссии и нормативно-методическими документами ФСТЭК России

Практическое занятие 10

Вид практического занятия: смешанная форма практического занятия.

Образовательные технологии: групповая дискуссия

Тема и содержание практического занятия: Перечень основных документов ФСТЭК РФ по вопросам защиты информации. Основные положения концепции защиты СВТ и АС от НСД к информации. Принципы защиты от НСД. Построение модели нарушителя безопасности АС. Система разграничения доступа (СРД) и её функции. Средства для СРД. Реализация СРД. Проверка выполнения технических требований по защите. Сертификат соответствия СВТ или АС требованиям по защите.

Цель работы: получить практические знания и навыки по защите СВТ и АС от НСД.

Учебные вопросы:

- Перечень основных документов ФСТЭК РФ по вопросам защиты информации. Основные положения концепции защиты СВТ и АС от НСД к информации.
- Определение НСД к информации. Два направления защиты от НСД. Особенности функций защиты в СВТ и АС. Основные способы НСД. Принципы защиты от НСД.
- Построение модели нарушителя безопасности АС. Уровни возможностей, предоставляемые нарушителям штатными средствами АС и СВТ.
- Характеристики оценки технических средств защиты от НСД. Система разграничения доступа (СРД) и её функции. Средства для СРД.

- Реализация СРД. Проверка выполнения технических требований по защите. Сертификат соответствия СВТ или АС требованиям по защите.
- Продолжительность практического занятия-2 часа

3. Указания по проведению лабораторных работ.

Цель и задачи выполнения лабораторных работ: Определение порядка и последовательности действий по обоснованию предложений руководителю по результатам анализа и прогноза по заданной ситуации.

Методика *определяется моделью соответствующей задачи, решаемой обучающимся на занятии по заданию преподавателя)* и средства *для* выполнения лабораторных работ: общее *программное обеспечение*

Этапы выполнения лабораторных работ *(Постановка задачи лабораторной работы. Ознакомление обучающегося с содержанием и объемом лабораторной работы. Порядок выполнения лабораторной работы. Регистрация результатов и оформление отчета о лабораторной работе. Заключительная часть лабораторной работы).*

Тематика лабораторных работ и задания к ним *(тематика лабораторных работ должна соответствовать рабочей программе дисциплины).*

Лабораторная работа № 1.

Тема: Структура информационных ресурсов и администрирование в компьютерных системах

Цель занятия**:** Определение конфигурации информационных ресурсов компьютерных систем. Администрирование в компьютерных системах.

Продолжительность практического занятия-0.5 часа

Задание.

ЗАДАНИЕ № 1

Тема: Теоретические аспекты проведения специальных исследований (СИ) на предприятии

Цель работы.

Изучение основных принципов проведения специальных исследований на предприятии. Освоить структуру ведения общей теоретической части проведения специальных исследований.

Продолжительность занятия: полтора учебных часа.

Задания.

1.Изучить теоретическую часть Задания №1.

2.Выполнить практическую часть Задания №1:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

3. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Специальные исследования (спец. исследования, СИ) — комплекс действий, направленный на обнаружение потенциальных технических каналов утечки защищаемой информации с помощью специального контрольно-измерительного оборудования, в соответствии с нормативно-методическими документами ФСБ России и ФСТЭК России.

Проведение спец. исследований определяет возможность считывания и перехвата сигнала специальными средствами разведки в рамках определённых границ (защищённость утечек по каналам ПЭМИН — побочные электромагнитные излучения и наводки).

Введем для большей ясности определения, связанные с основой ведения спец. исследований на предприятии. Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается ценная информация.

Автоматизированная система (АС) – устройство или комплекс устройств, необходимых для передачи, хранения и обработки конфиденциальной информации, прошедшая процедуру аттестации в соответствии с законодательством РФ.

Контролируемая зона (КЗ) – пространство, в котором исключено неконтролируемое пребывание посторонних лиц или сотрудников, не имеющих прямое отношение к данному пространству. Примерами могут послужить: периметр охраняемой территории; ограждающие конструкции охраняемого здания или охраняемой территории.

Информационный сигнал – электрические сигналы, акустические, электромагнитные и т.д., по параметрам которых можно раскрыть конфиденциальную информацию, передаваемую, хранимую или обрабатываемую в ос-

новных технических средствах и системах или обсуждаемая в защищенном исполнении.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для обработки, хранения и передачи конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

Средства активной защиты информации по каналам ПЭМИН (САЗ) – технические средства формирования маскирующих электромагнитных помех в местах возможного съема защищаемой информации, прошедшие обязательную процедуру сертификации по линии ФСТЭК России.

Деятельность по технической защите конфиденциальной информации (ТЗКИ) – выполнение работ и (или) оказание услуг по ее защите:

– от несанкционированного доступа,

– от утечки по техническим каналам,

– от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Важно! Данный вид деятельности является лицензируемым. Лицензирование деятельности по ТЗКИ осуществляет ФСТЭК России.

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные поля, создаваемые в окружающем пространстве СВТ, специально для этого не предназначенными (в случае ПЭМИ) или наводки данных излучений на токоведущие конструкции, линии и подключенные к ним ТС.

Существует несколько видов проведения специсследований на определенные ТС. В данном случае это акустоэлектрическое преобразование (АЭП) и ПЭМИН. В случае АЭП исследуемое средство подвергается воздействию

некоих акустических частот. Из этого обосновывается определенный вывод о возможности использования ТС на невозможности подверженности АЭП.

Как уже было указано в определениях, ПЭМИ создаются вокруг работающих технических средств, которые специально для данного излучения не создавались. То есть излучение от радиопередатчиков, мобильных телефонов – это не побочные излучения. А вот излучения при работе компьютера от монитора, принтера, накопителей информации являются побочными.

Если вспомнить физику, то вокруг проводника, по которому протекает электрический ток возникает электромагнитное поле. Если по данному проводнику передается какой-либо сигнал, то, следовательно, и электромагнитное поле тоже будет изменяться по тем же законам, что и сигнал, протекающий в линии. Таким образом, источником сигнала ПЭМИ являются все токоведущие линии в ТС, по которым в процессе работы передаются какие-либо сигналы.

Как известно электромагнитные поля могут распространяться на значительные расстояния и конструкции помещений тому не преграда. Скорость передачи данных и обработки информации в современных средствах вычислительной техники постоянно растет, а значит растут и частоты сигналов ПЭМИ. Частоты сигналов ПЭМИ могут начинаться от единиц кГц и заканчиваться единицами ГГц, а гармоники этих сигналов могут находиться еще выше по частоте.

Если вспомнить, что в проводнике, помещенном в электромагнитное поле, возникает электрический ток, то очевидно, что могут возникать наводки ПЭМИ на любые токоведущие элементы (систему отопления, короб системы вентиляции и т. д.), в том числе и любые линии и ТС, подключенные к ним, попадающие под действие данного электромагнитного поля.

Перехват этой информации можно осуществить путем анализа изменений параметров ПЭМИН с помощью специальных высокочувствительных радиоприемных устройств, оснащенных специализированными антеннами, пробниками напряжения, токосъемниками.

На (рис. 1) приведена физика утечки информации за счет ПЭМИ.

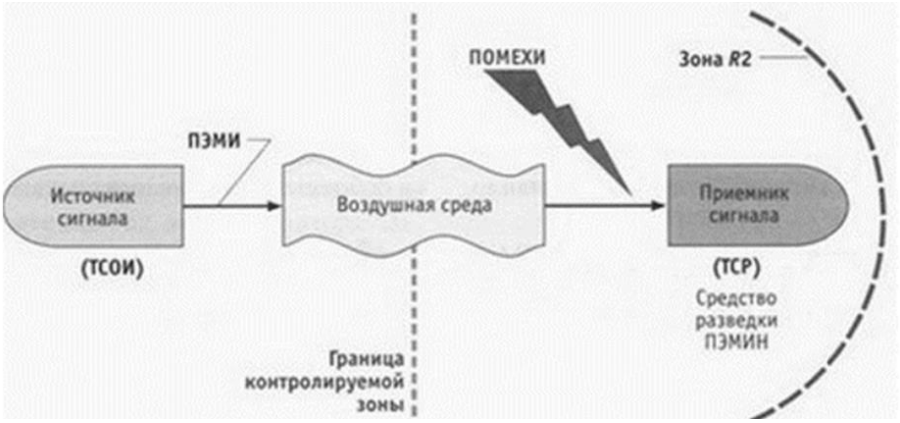


Рисунок 1. Схема ТКУИ за счет ПЭМИ

На (рис. 2) приведена физика утечки информации за счет ПЭМИН.

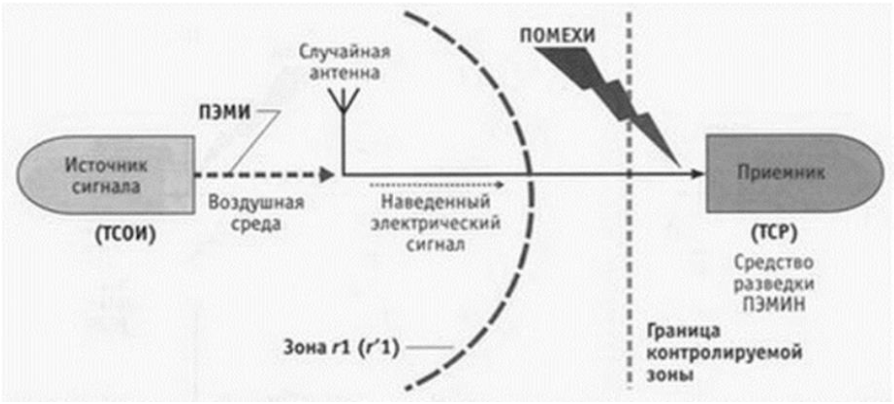


Рисунок 2. Схема ТКУИ за счет ПЭМИН

Поясним некоторые сокращения и термины на схемах:

- ТСОИ – технические средства обработки информации (все что попадает под определение ОТСС);
- ТСР–технические средства разведки;
- зона R2 – расстояние, на котором возможен перехват защищаемой информации за счет ПЭМИ;
- зона r1(r'1) – расстояние, наличие в пределах которого случайных антенн (токоведущие конструкции, линии и ТС) создает возможность утечки информации за счет наводок ПЭМИ.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенной случайной антенной может являться стационарный те-

лефон, датчик пожарной сигнализации, громкоговоритель, подключенная к линии, выходящей за пределы КЗ.

Распределенные случайные антенным – антенны с распределенными параметрами. К ним можно отнести: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ.

Также разделяют саму информации по каналам АЭП и ПЭМИ на случай информативности. Информативные – сигналы с несущей, модулированной информативным сигналом. Примером могут послужить: сигнал от флэш-накопителя USB; VGA-интерфейс монитора; и т.д.

Неинформативные сигналы – сигналы, анализ которых не дает представления об обрабатываемой информации. Примеры: излучения от работы источников питания в узлах ТС; сигнал обработки режимов видеокартой; и т.д.

Важно! Всё приведенное выше относится к составной части по проведению работ, связанных с специальными исследованиями ОТСС и ВТСС. Однако это лишь малая часть того, что можно было бы изложить. Остальная теоретическая и прикладная часть изучается непосредственно работником предприятия в режимно секретном подразделении. Все методические материалы работ, связанных с проведением специальных исследований имеют грифы СЕКРЕТНО и СОВЕРШЕННО СЕКРЕТНО. Вышеизложенный материал является открытым и считается опорным в общих знаниях ТЗИ.

Практическая часть.

Вопросы для самопроверки:

16) Дайте определение специальным исследованиям в рамках данного учебного занятия.
17) Какие и сколько существует грифов секретности в рамках законодательства РФ?
18) Что такое зона r1(r’1) в ТЗИ?
19) Дайте определение ОТСС и ВТСС и в чем их различие?

20) На какие категории разбиваются случайные антенны в КЗ и в чем их разница? И на какие категории разбиваются информационные сигналы и в чем их разница?

Практические задания:

7) Опишите собственными словами следующие определения. ОТСС; ВТСС; ТКУИ.
8) В соответствии с (рис. 1) данного учебного задания, источником распространения сигнала ПЭМИ между техническим средством и техническим средством разведки является воздушная среда. Что будет если изменить воздушную среду на более плотную, а что, если перенести её в вакуум. Ответ обоснуйте.

Однажды, двое ученых задались очень интересной задачей, связанной с передачей информативного сигнала технического средства через канал ПЭМИ по очень интересной схеме. У них получилось и даже на современном этапе злоумышленники охотно придают значение данному средству получения заведомо важной для них информации. Двух ученых звали Маркус Кун и Росс Андерсон. При помощи сети Интернет, найдите информацию о данной процедуре получения информативного сигнала по каналу ПЭМИ и расскажите в общих чертах об этой технологии

ЗАДАНИЕ № 2

Тема: Теоретические основы средств измерения программно-аппаратных комплексов (ПАК) и альтернативной измерительной площадки (АИП)

Цель работы.

Изучение теоретической основы средств измерений сигналов. Освоить особенности поиска и идентификации сигналов при помощи альтернативной измерительной площадки.

Продолжительность занятия: полтора учебных часа.

Задания.

19. Изучить теоретическую часть Задания №2.
20. Выполнить практическую часть Задания №2:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

21. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

В связи с тем, что многие организации, занимающиеся производством и распространением программно-аппаратных комплексов, предлагают на рынке целые линейки своих продуктов, отличающихся только аппаратной частью (анализаторы спектра) и соответственно ценой на данные товары в этой линейке. На рынке представлены программ- но-аппаратные комплексы следующих производителей, распространителей: «Навигатор ПхГ» – «НЕЛК», «Сигурд Мх» – «МАСКОМ», «Легенда» – «АВМ-СИСТЕМС». Стоит отметить, что все комплексы, рассматриваемые в данной работе, имеют сертификаты ФСТЭК России и метрологический сертификат соответствия на измерительное оборудование. Пример ПАК представлен на (рис. 1).

Рисунок 1. ПАК «Сигурд М18»

Требования к антеннам.

В полосе частот от 200 Гц до 30 МГц в комплект антенн должны входить магнитная и (или) электрическая антенны.

Для измерения магнитной составляющей электромагнитного поля, антенна должна быть: электрически экранированной рамочной антенной, имеющей такие размеры, чтобы ее рамка помещалась в квадрат со стороной не более 0,6 м, или ферритовая антенна длиной не более 0,5 м.

Допускаемая погрешность измерений напряженности магнитного поля (измеритель с магнитной антенной) не должна превышать 2,5 дБ.

Конструкция антенн (антенного штатива) должна обеспечивать возможность плавного изменения высоты расположения антенны над землей от 0,8 м до 1,25 м, а также возможность поворота магнитной и электрической антенн на 360° вокруг оси.

В полосе частот от 30 до 1000 МГц в комплект антенн должны входить одна или несколько электрических антенн одного из следующих типов:

а) линейный симметричный вибратор на полосу частот от 30 до 80 МГц, размер которого равен длине полуволнового симметричного вибратора на частоте 80 МГц, и настраиваемый полуволновой симметричный вибратор в полосе частот от 80 до 1000 МГц, имеющий КСВН не более 2,5;

б) биконическая антенна, максимальный размер которой должен быть не более 1,35 м в полосе частот от 30 до 300 МГц и с КСВН не более 3,0, и биконическая антенна, максимальный размер которой – не более 0,5 м в полосе частот от 300 до 1000 МГц с КСВН не более 2,5;

в) широкополосная антенна, главный лепесток диаграммы направленности которой должен быть таким, чтобы в направлении непосредственного излучения от источника ПЭМИН и в направлении отраженного от земли луча разность коэффициентов усиления антенны не превышала бы 1 дБ, с КСВН не более 2,5.

Конструкция антенны (антенного штатива) должна обеспечивать возможность плавного изменения высоты центра симметрии над землей от 1 до

4 м и поворота вокруг горизонтальной оси на 180°, а также фиксированную ориентацию в трех взаимно ортогональных направлениях.

Допускаемая погрешность измерений напряженности электрического поля (измеритель с биконической, электрической антенной) не должна превышать 2,5 дБ на частотах до 1000 МГц.

Антенны должны иметь коэффициент калибровки, позволяющий измерять уровни полей. Рекомендуемый коэффициент калибровки антенн – не более 40 дБ. Погрешность коэффициента калибровки антенн должна быть не более 2 дБ.

Требования к анализатору.

Должен иметь несимметричный вход с номинальным значением сопротивления 50 Ом с коэффициентом стоячей волны по напряжению (КСВН) не более 2 при ослаблении входного аттенюатора 0 дБ и не более 1,2 при ослаблении входного аттенюатора 10 дБ и более.

Измерители совместно с первичными преобразователями должны обеспечивать измерения характеристик ПЭМИ в децибелах, относительно 1 мкВ, 1 мкА, 1 мкВ/м, 1 мкА/м, 1 мВт/м2.

Анализатор спектра должен быть программируемым, для дистанционного управления, т. е. должен обрабатывать команды, которые ему посылает ПЭВМ.

Должен иметь интерфейсы LAN или USB, или GPIB, или RS-232 для передачи данных с ПЭВМ на анализатор спектра и обратно.

Анализатор спектра должен иметь квазипиковый, пиковый и со среднеквадратичным отклонением детекторы.

Работать в полосе частот 9 кГц...1000 МГц.

Иметь полосы пропускания в диапазоне 1 кГц...3 МГц. Погрешность, вносимая собственными шумами, должна быть не более 1 дБ. Анализатор спектра должен обеспечивать звуковой контроль ПЭМИ, имеющих амплитудную и частотную (на частотах свыше 30 МГц) модуляцию, с помощью встроенных или подключаемых приборов или устройств.

Примерный перечень оборудования приведен в (табл. 1).

Таблица 1. Перечень оборудования для проведения оценки защищенности по каналу ПЭМИН

Наименование средств измерения	Тип	Диапазон частот
Анализатор спектра	LIGNext1 NS-30A	10 кГц -3 ГГц
Антенна магнитная рамочная активная	Н-30	10 Гц – 30 МГц
Антенна электрическая дипольная активная	Е-3000	30 МГц – 3000 МГц
Антенна электрическая дипольная активная	Е-30	10 Гц – 30 МГц
Пробник напряжения	П-400	10 Гц – 300 МГц
Осциллограф	LeCroy Wavesurfer 62Xs	0 Гц – 600 МГц
Генератор сигналов	Г4-218	200 кГц-1 ГГц

Альтернативная измерительная площадка.

Временная методика оценки защищенности ОТСС, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации (КИ), описанная в «Сборнике временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам» предполагает собой поиск и измерение опасных сигналов непосредственно на объекте информатизации.

Однако, шумовая обстановка на объекте информатизации весьма нестабильна. Помимо нестабильности она абсолютно неисследованная. Оператор при проведении измерений может столкнуться с таким явлением как «стоячая волна».

Стоячая волна (электромагнитная) – периодическое изменение амплитуды напряженности электрического и магнитного полей вдоль направления

распространения, вызванное интерференцией, падающей и отраженной волн. Например, стоячая волна возникает при отражении волны от преград и неоднородностей в результате взаимодействия (интерференции), падающей и отражённой волн.

Присутствие такой волны во время проведения измерений однозначно приведёт к ошибке.

Измерительная площадка – площадка, отвечающая требованиям, обеспечивающим правильное измерение уровней индустриальных радиопомех (ИРП), излучаемых ТС в регламентированных условиях. Видов ИП предусматриваются два – «открытая измерительная площадка» и «альтернативная измерительная площадка». Поскольку строительство и эксплуатация открытой площадки весьма дорого, сосредоточимся на более дешёвом варианте – АИП. Разница между открытой ИП и АИП заключается в том, что последняя должна размещаться не в открытом пространстве, а в некотором помещении, в здании. При том физические характеристики АИП (прежде всего «затухание» электромагнитного поля) должны оставаться в пределах установленного допуска.

Важно! Перед вводом в эксплуатацию АИП оценивается минимум искажений, вносимых в распределение электромагнитного поля ограждающими конструкциями помещения, который можно допустить. Иными словами, оператор заранее знает о наличии и характере «стоячих волн» и о характеристиках закона затухания электромагнитного поля. Это позволяет получать информацию об «опасных» информативных сигналах корректнее, чем на ОИ, на котором абсолютно не исследована шумовая обстановка.

Практическая часть.

Вопросы для самопроверки:

16) Назовите весь перечень оборудования для проведения оценки защищенности по ПЭМИ.

17) Дайте определение измерительной площадки в рамках данного задания.
18) Сколько существует видов измерительных площадок (ИП) и в чем их различие?
19) На сколько метров минимально и максимально предполагается плавное размещение антенны по высоте?
20) Какой должен быть коэффициент калибровки у антенн?

Практические задания:

7) Как по Вашему мнению вы представляете себе открытую измерительную площадку и альтернативную? Опишите их. В чем их основное различие? Ответ обоснуйте.
8) Представьте, что Вы начинающий сотрудник предприятия ООО «НПП «ИБЦ». Начался ваш седьмой рабочий день. Вы в обычном распорядке, получив задание, идете включать лабораторное автоматизированное рабочее место и ПАК. Неожиданным образом узнаёте, что откалиброванная антенна начала давать сбой. Вы (без особой паники) начинаете искать пути решения. По Вашему мнению, каковы основные три шага на пути решения этой проблемы? Ответ обоснуйте.

Лабораторная работа № 2.
Тема: Анализ угроз информационной безопасности
Цель занятия: Факторы, воздействующие на защищаемую информацию. Классификация угроз. Естественные и искусственные угрозы. Основные направления и методы реализации угроз.
Основные виды атак на КС, их классификация. Проблемы обеспечения информационной безопасности в проводных КС.
Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.
Продолжительность практического занятия-0.5 часа
Задание.

ЗАДАНИЕ № 1

Тема: Теоретические аспекты проведения специальных исследований (СИ) на предприятии

Цель работы.

Изучение основных принципов проведения специальных исследований на предприятии. Освоить структуру ведения общей теоретической части проведения специальных исследований.

Продолжительность занятия: полтора учебных часа.

Задания.

22. Изучить теоретическую часть Задания №1.
23. Выполнить практическую часть Задания №1:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

24. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Специальные исследования (специсследования, СИ) — комплекс действий, направленный на обнаружение потенциальных технических каналов утечки защищаемой информации с помощью специального контрольно-измерительного оборудования, в соответствии с нормативно-методическими документами ФСБ России и ФСТЭК России.

Проведение специсследований определяет возможность считывания и перехвата сигнала специальными средствами разведки в рамках определённых границ (защищённость утечек по каналам ПЭМИН — побочные электромагнитные излучения и наводки).

Введем для большей ясности определения, связанные с основой ведения специсследований на предприятии. Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической сре-

ды распространения информативного сигнала и средств, которыми добывается ценная информация.

Автоматизированная система (АС) – устройство или комплекс устройств, необходимых для передачи, хранения и обработки конфиденциальной информации, прошедшая процедуру аттестации в соответствии с законодательством РФ.

Контролируемая зона (КЗ) – пространство, в котором исключено неконтролируемое пребывание посторонних лиц или сотрудников, не имеющих прямое отношение к данному пространству. Примерами могут послужить: периметр охраняемой территории; ограждающие конструкции охраняемого здания или охраняемой территории.

Информационный сигнал – электрические сигналы, акустические, электромагнитные и т.д., по параметрам которых можно раскрыть конфиденциальную информацию, передаваемую, хранимую или обрабатываемую в основных технических средствах и системах или обсуждаемая в защищенном исполнении.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для обработки, хранения и передачи конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

Средства активной защиты информации по каналам ПЭМИН (САЗ) – технические средства формирования маскирующих электромагнитных помех в местах возможного съема защищаемой информации, прошедшие обязательную процедуру сертификации по линии ФСТЭК России.

Деятельность по технической защите конфиденциальной информации (ТЗКИ) – выполнение работ и (или) оказание услуг по ее защите:

– от несанкционированного доступа,

– от утечки по техническим каналам,

– от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Важно! Данный вид деятельности является лицензируемым. Лицензирование деятельности по ТЗКИ осуществляет ФСТЭК России.

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные поля, создаваемые в окружающем пространстве СВТ, специально для этого не предназначенными (в случае ПЭМИ) или наводки данных излучений на токоведущие конструкции, линии и подключенные к ним ТС.

Существует несколько видов проведения специсследований на определенные ТС. В данном случае это акустоэлектрическое преобразование (АЭП) и ПЭМИН. В случае АЭП исследуемое средство подвергается воздействию некоих акустических частот. Из этого обосновывается определенный вывод о возможности использования ТС на невозможности подверженности АЭП.

Как уже было указано в определениях, ПЭМИ создаются вокруг работающих технических средств, которые специально для данного излучения не создавались. То есть излучение от радиопередатчиков, мобильных телефонов – это не побочные излучения. А вот излучения при работе компьютера от монитора, принтера, накопителей информации являются побочными.

Если вспомнить физику, то вокруг проводника, по которому протекает электрический ток возникает электромагнитное поле. Если по данному проводнику передается какой-либо сигнал, то, следовательно, и электромагнитное поле тоже будет изменяться по тем же законам, что и сигнал, протекающий в линии. Таким образом, источником сигнала ПЭМИ являются все токоведущие линии в ТС, по которым в процессе работы передаются какие-либо сигналы.

Как известно электромагнитные поля могут распространяться на значительные расстояния и конструкции помещений тому не преграда. Скорость передачи данных и обработки информации в современных средствах вычис-

лительной техники постоянно растет, а значит растут и частоты сигналов ПЭМИ. Частоты сигналов ПЭМИ могут начинаться от единиц кГц и заканчиваться единицами ГГц, а гармоники этих сигналов могут находиться еще выше по частоте.

Если вспомнить, что в проводнике, помещенном в электромагнитное поле, возникает электрический ток, то очевидно, что могут возникать наводки ПЭМИ на любые токоведущие элементы (систему отопления, короб системы вентиляции и т. д.), в том числе и любые линии и ТС, подключенные к ним, попадающие под действие данного электромагнитного поля.

Перехват этой информации можно осуществить путем анализа изменений параметров ПЭМИН с помощью специальных высокочувствительных радиоприемных устройств, оснащенных специализированными антеннами, пробниками напряжения, токосъемниками.

На (рис. 1) приведена физика утечки информации за счет ПЭМИ.

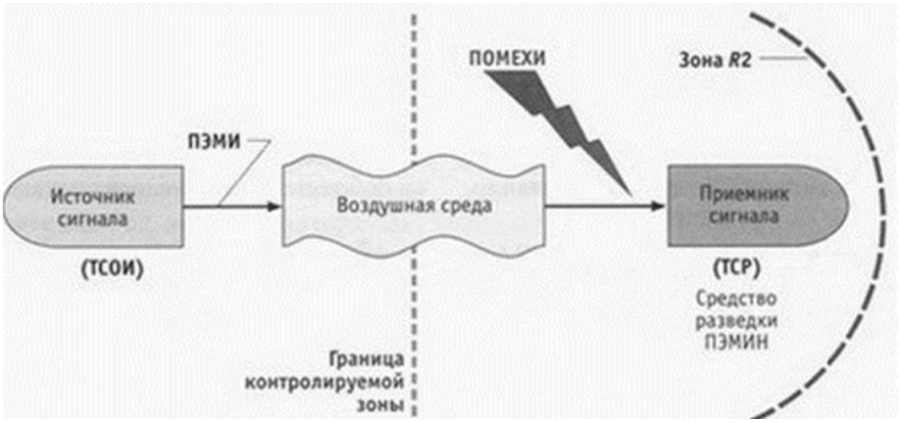


Рисунок 1. Схема ТКУИ за счет ПЭМИ

На (рис. 2) приведена физика утечки информации за счет ПЭМИН.

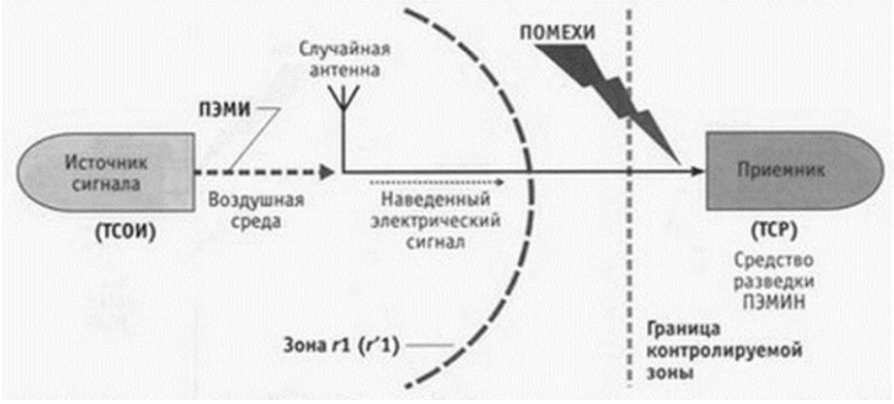


Рисунок 2. Схема ТКУИ за счет ПЭМИН

Поясним некоторые сокращения и термины на схемах:

- ТСОИ – технические средства обработки информации (все что попадает под определение ОТСС);
- ТСР–технические средства разведки;
- зона R2 – расстояние, на котором возможен перехват защищаемой информации за счет ПЭМИ;
- зона r1(r'1) – расстояние, наличие в пределах которого случайных антенн (токоведущие конструкции, линии и ТС) создает возможность утечки информации за счет наводок ПЭМИ.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенной случайной антенной может являться стационарный телефон, датчик пожарной сигнализации, громкоговоритель, подключенная к линии, выходящей за пределы КЗ.

Распределенные случайные антенным – антенны с распределенными параметрами. К ним можно отнести: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ.

Также разделяют саму информации по каналам АЭП и ПЭМИ на случай информативности. Информативные – сигналы с несущей, модулированной информативным сигналом. Примером могут послужить: сигнал от флэш-накопителя USB; VGA-интерфейс монитора; и т.д.

Неинформативные сигналы – сигналы, анализ которых не дает представления об обрабатываемой информации. Примеры: излучения от работы источников питания в узлах ТС; сигнал обработки режимов видеокартой; и т.д.

Важно! Всё приведенное выше относится к составной части по проведению работ, связанных с специальными исследованиями ОТСС и ВТСС. Однако это лишь малая часть того, что можно было бы изложить. Остальная теоретическая и прикладная часть изучается непосредственно работником предприятия в режимно секретном подразделении. Все методические мате-

риалы работ, связанных с проведением специальных исследований имеют грифы СЕКРЕТНО и СОВЕРШЕННО СЕКРЕТНО. Вышеизложенный материал является открытым и считается опорным в общих знаниях ТЗИ.

Практическая часть.

Вопросы для самопроверки:

Дайте определение специальным исследованиям в рамках данного учебного занятия.

Какие и сколько существует грифов секретности в рамках законодательства РФ?

Что такое зона r1(r'1) в ТЗИ?

Дайте определение ОТСС и ВТСС и в чем их различие?

На какие категории разбиваются случайные антенны в КЗ и в чем их разница? И на какие категории разбиваются информационные сигналы и в чем их разница?

Практические задания:

Опишите собственными словами следующие определения. ОТСС; ВТСС; ТКУИ.

В соответствии с (рис. 1) данного учебного задания, источником распространения сигнала ПЭМИ между техническим средством и техническим средством разведки является воздушная среда. Что будет если изменить воздушную среду на более плотную, а что, если перенести её в вакуум. Ответ обоснуйте.

Однажды, двое ученых задались очень интересной задачей, связанной с передачей информативного сигнала технического средства через канал ПЭМИ по очень интересной схеме. У них получилось и даже на современном этапе злоумышленники охотно придают значение данному средству получения заведомо важной для них информации. Двух ученых звали Маркус Кун и Росс Андерсон. При помощи сети Интернет, найдите информацию о данной процедуре получения информативного сигнала по каналу ПЭМИ и расскажите в общих чертах об этой технологии

ЗАДАНИЕ № 2

Тема: Теоретические основы средств измерения программно-аппаратных комплексов (ПАК) и альтернативной измерительной площадки (АИП)

Цель работы.

Изучение теоретической основы средств измерений сигналов. Освоить особенности поиска и идентификации сигналов при помощи альтернативной измерительной площадки.

Продолжительность занятия: полтора учебных часа.

Задания.

Изучить теоретическую часть Задания №2.

Выполнить практическую часть Задания №2:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

В связи с тем, что многие организации, занимающиеся производством и распространением программно-аппаратных комплексов, предлагают на рынке целые линейки своих продуктов, отличающихся только аппаратной частью (анализаторы спектра) и соответственно ценой на данные товары в этой линейке. На рынке представлены программ- но-аппаратные комплексы следующих производителей, распространителей: «Навигатор ПхГ» – «НЕЛК», «Сигурд Мх» – «МАСКОМ», «Легенда» – «АВМ-СИСТЕМС». Стоит отметить, что все комплексы, рассматриваемые в данной работе, имеют сертификаты ФСТЭК России и метрологический сертификат соответствия на измерительное оборудование. Пример ПАК представлен на (рис. 1).

Рисунок 1. ПАК «Сигурд М18»

Требования к антеннам.

В полосе частот от 200 Гц до 30 МГц в комплект антенн должны входить магнитная и (или) электрическая антенны.

Для измерения магнитной составляющей электромагнитного поля, антенна должна быть: электрически экранированной рамочной антенной, имеющей такие размеры, чтобы ее рамка помещалась в квадрат со стороной не более 0,6 м, или ферритовая антенна длиной не более 0,5 м.

Допускаемая погрешность измерений напряженности магнитного поля (измеритель с магнитной антенной) не должна превышать 2,5 дБ.

Конструкция антенн (антенного штатива) должна обеспечивать возможность плавного изменения высоты расположения антенны над землей от 0,8 м до 1,25 м, а также возможность поворота магнитной и электрической антенн на 360° вокруг оси.

В полосе частот от 30 до 1000 МГц в комплект антенн должны входить одна или несколько электрических антенн одного из следующих типов:

а) линейный симметричный вибратор на полосу частот от 30 до 80 МГц, размер которого равен длине полуволнового симметричного вибратора

на частоте 80 МГц, и настраиваемый полуволновой симметричный вибратор в полосе частот от 80 до 1000 МГц, имеющий КСВН не более 2,5;

б) биконическая антенна, максимальный размер которой должен быть не более 1,35 м в полосе частот от 30 до 300 МГц и с КСВН не более 3,0, и биконическая антенна, максимальный размер которой – не более 0,5 м в полосе частот от 300 до 1000 МГц с КСВН не более 2,5;

в) широкополосная антенна, главный лепесток диаграммы направленности которой должен быть таким, чтобы в направлении непосредственного излучения от источника ПЭМИН и в направлении отраженного от земли луча разность коэффициентов усиления антенны не превышала бы 1 дБ, с КСВН не более 2,5.

Конструкция антенны (антенного штатива) должна обеспечивать возможность плавного изменения высоты центра симметрии над землей от 1 до 4 м и поворота вокруг горизонтальной оси на 180°, а также фиксированную ориентацию в трех взаимно ортогональных направлениях.

Допускаемая погрешность измерений напряженности электрического поля (измеритель с биконической, электрической антенной) не должна превышать 2,5 дБ на частотах до 1000 МГц.

Антенны должны иметь коэффициент калибровки, позволяющий измерять уровни полей. Рекомендуемый коэффициент калибровки антенн – не более 40 дБ. Погрешность коэффициента калибровки антенн должна быть не более 2 дБ.

Требования к анализатору.

Должен иметь несимметричный вход с номинальным значением сопротивления 50 Ом с коэффициентом стоячей волны по напряжению (КСВН) не более 2 при ослаблении входного аттенюатора 0 дБ и не более 1,2 при ослаблении входного аттенюатора 10 дБ и более.

Измерители совместно с первичными преобразователями должны обеспечивать измерения характеристик ПЭМИ в децибелах, относительно 1 мкВ, 1 мкА, 1 мкВ/м, 1 мкА/м, 1 мВт/м2.

Анализатор спектра должен быть программируемым, для дистанционного управления, т. е. должен обрабатывать команды, которые ему посылает ПЭВМ.

Должен иметь интерфейсы LAN или USB, или GPIB, или RS-232 для передачи данных с ПЭВМ на анализатор спектра и обратно.

Анализатор спектра должен иметь квазипиковый, пиковый и со среднеквадратичным отклонением детекторы.

Работать в полосе частот 9 кГц...1000 МГц.

Иметь полосы пропускания в диапазоне 1 кГц...3 МГц. Погрешность, вносимая собственными шумами, должна быть не более 1 дБ. Анализатор спектра должен обеспечивать звуковой контроль ПЭМИ, имеющих амплитудную и частотную (на частотах свыше 30 МГц) модуляцию, с помощью встроенных или подключаемых приборов или устройств.

Примерный перечень оборудования приведен в (табл. 1).

Таблица 1. Перечень оборудования для проведения оценки защищенности по каналу ПЭМИН

Наименование средств измерения	Тип	Диапазон частот
Анализатор спектра	LIGNext1 NS-30A	10 кГц -3 ГГц
Антенна магнитная рамочная активная	Н-30	10 Гц – 30 МГц
Антенна электрическая дипольная активная	Е-3000	30 МГц – 3000 МГц
Антенна электрическая дипольная активная	Е-30	10 Гц – 30 МГц
Пробник напряжения	П-400	10 Гц – 300 МГц
Осциллограф	LeCroy Wavesurfer 62Xs	0 Гц – 600 МГц
Генератор сигналов	Г4-218	200 кГц-1 ГГц

Альтернативная измерительная площадка.

Временная методика оценки защищенности ОТСС, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации (КИ), описанная в «Сборнике временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам» предполагает собой поиск и измерение опасных сигналов непосредственно на объекте информатизации.

Однако, шумовая обстановка на объекте информатизации весьма нестабильна. Помимо нестабильности она абсолютно неисследованная. Оператор при проведении измерений может столкнуться с таким явлением как «стоячая волна».

Стоячая волна (электромагнитная) – периодическое изменение амплитуды напряженности электрического и магнитного полей вдоль направления распространения, вызванное интерференцией, падающей и отраженной волн. Например, стоячая волна возникает при отражении волны от преград и неоднородностей в результате взаимодействия (интерференции), падающей и отражённой волн.

Присутствие такой волны во время проведения измерений однозначно приведёт к ошибке.

Измерительная площадка – площадка, отвечающая требованиям, обеспечивающим правильное измерение уровней индустриальных радиопомех (ИРП), излучаемых ТС в регламентированных условиях. Видов ИП предусматриваются два – «открытая измерительная площадка» и «альтернативная измерительная площадка». Поскольку строительство и эксплуатация открытой площадки весьма дорого, сосредоточимся на более дешёвом варианте – АИП. Разница между открытой ИП и АИП заключается в том, что последняя должна размещаться не в открытом пространстве, а в некотором помещении, в здании. При том физические характеристики АИП (прежде всего «затухание» электромагнитного поля) должны оставаться в пределах установленного допуска.

Важно! Перед вводом в эксплуатацию АИП оценивается минимум искажений, вносимых в распределение электромагнитного поля ограждающими конструкциями помещения, который можно допустить. Иными словами, оператор заранее знает о наличии и характере «стоячих волн» и о характеристиках закона затухания электромагнитного поля. Это позволяет получать информацию об «опасных» информативных сигналах корректнее, чем на ОИ, на котором абсолютно не исследована шумовая обстановка.

Практическая часть.

Вопросы для самопроверки:

Назовите весь перечень оборудования для проведения оценки защищенности по ПЭМИ.

Дайте определение измерительной площадки в рамках данного задания.

Сколько существует видов измерительных площадок (ИП) и в чем их различие?

На сколько метров минимально и максимально предполагается плавное размещение антенны по высоте?

Какой должен быть коэффициент калибровки у антенн?

Практические задания:

Как по Вашему мнению вы представляете себе открытую измерительную площадку и альтернативную? Опишите их. В чем их основное различие? Ответ обоснуйте.

Представьте, что Вы начинающий сотрудник предприятия ООО «НПП «ИБЦ». Начался ваш седьмой рабочий день. Вы в обычном распорядке, получив задание, идете включать лабораторное автоматизированное рабочее место и ПАК. Неожиданным образом узнаёте, что откалиброванная антенна начала давать сбой. Вы (без особой паники)

начинаете искать пути решения. По Вашему мнению, каковы основные три шага на пути решения этой проблемы? Ответ обоснуйте.

Лабораторная работа № 3.
Тема: Основные уровни защиты информации в компьютерных системах
Цель занятия: Методы и средства обеспечения защиты информации в компьютерных системах. Защита представления информации. Защита содержания информации.
Сертификация программных и программно-технических средств защиты конфиденциальной компьютерной информации.
Методы обеспечения защиты информации – препятствие, маскировка, управление доступом. Функции защиты при управлении доступом. Принуждение и побуждение.
Физические средства защиты компьютерных систем. Нейтрализация утечки информации по электромагнитным каналам – применение генераторов шума. Защита от наводок. Аппаратные средства защиты в КС. Задачи, решаемые программными средствами защиты.
Продолжительность практического занятия-0.5 часа
Задание.

ЗАДАНИЕ № 1

Тема: Теоретические аспекты проведения специальных исследований (СИ) на предприятии

Цель работы.

Изучение основных принципов проведения специальных исследований на предприятии. Освоить структуру ведения общей теоретической части проведения специальных исследований.

Продолжительность занятия: полтора учебных часа.

Задания.

Изучить теоретическую часть Задания №1.

Выполнить практическую часть Задания №1:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Специальные исследования (специсследования, СИ) — комплекс действий, направленный на обнаружение потенциальных технических каналов утечки защищаемой информации с помощью специального контрольно-измерительного оборудования, в соответствии с нормативно-методическими документами ФСБ России и ФСТЭК России.

Проведение специсследований определяет возможность считывания и перехвата сигнала специальными средствами разведки в рамках определённых границ (защищённость утечек по каналам ПЭМИН — побочные электромагнитные излучения и наводки).

Введем для большей ясности определения, связанные с основой ведения специсследований на предприятии. Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается ценная информация.

Автоматизированная система (АС) – устройство или комплекс устройств, необходимых для передачи, хранения и обработки конфиденциальной информации, прошедшая процедуру аттестации в соответствии с законодательством РФ.

Контролируемая зона (КЗ) – пространство, в котором исключено неконтролируемое пребывание посторонних лиц или сотрудников, не имеющих прямое отношение к данному пространству. Примерами могут послужить: периметр охраняемой территории; ограждающие конструкции охраняемого здания или охраняемой территории.

Информационный сигнал – электрические сигналы, акустические, электромагнитные и т.д., по параметрам которых можно раскрыть конфиденциальную информацию, передаваемую, хранимую или обрабатываемую в основных технических средствах и системах или обсуждаемая в защищенном исполнении.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для обработки, хранения и передачи конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

Средства активной защиты информации по каналам ПЭМИН (САЗ) – технические средства формирования маскирующих электромагнитных помех в местах возможного съема защищаемой информации, прошедшие обязательную процедуру сертификации по линии ФСТЭК России.

Деятельность по технической защите конфиденциальной информации (ТЗКИ) – выполнение работ и (или) оказание услуг по ее защите:

– от несанкционированного доступа,

– от утечки по техническим каналам,

– от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Важно! Данный вид деятельности является лицензируемым. Лицензирование деятельности по ТЗКИ осуществляет ФСТЭК России.

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные поля, создаваемые в окружающем пространстве СВТ, специально для этого не предназначенными (в случае ПЭМИ) или наводки данных излучений на токоведущие конструкции, линии и подключенные к ним ТС.

Существует несколько видов проведения специсследований на определенные ТС. В данном случае это акустоэлектрическое преобразование (АЭП) и ПЭМИН. В случае АЭП исследуемое средство подвергается воздействию некоих акустических частот. Из этого обосновывается определенный вывод о возможности использования ТС на невозможности подверженности АЭП.

Как уже было указано в определениях, ПЭМИ создаются вокруг работающих технических средств, которые специально для данного излучения не создавались. То есть излучение от радиопередатчиков, мобильных телефонов – это не побочные излучения. А вот излучения при работе компьютера от монитора, принтера, накопителей информации являются побочными.

Если вспомнить физику, то вокруг проводника, по которому протекает электрический ток возникает электромагнитное поле. Если по данному проводнику передается какой-либо сигнал, то, следовательно, и электромагнитное поле тоже будет изменяться по тем же законам, что и сигнал, протекающий в линии. Таким образом, источником сигнала ПЭМИ являются все токоведущие линии в ТС, по которым в процессе работы передаются какие-либо сигналы.

Как известно электромагнитные поля могут распространяться на значительные расстояния и конструкции помещений тому не преграда. Скорость передачи данных и обработки информации в современных средствах вычислительной техники постоянно растет, а значит растут и частоты сигналов ПЭМИ. Частоты сигналов ПЭМИ могут начинаться от единиц кГц и заканчиваться единицами ГГц, а гармоники этих сигналов могут находиться еще выше по частоте.

Если вспомнить, что в проводнике, помещенном в электромагнитное поле, возникает электрический ток, то очевидно, что могут возникать наводки ПЭМИ на любые токоведущие элементы (систему отопления, короб системы вентиляции и т. д.), в том числе и любые линии и ТС, подключенные к ним, попадающие под действие данного электромагнитного поля.

Перехват этой информации можно осуществить путем анализа изменений параметров ПЭМИН с помощью специальных высокочувствительных радиоприемных устройств, оснащенных специализированными антеннами, пробниками напряжения, токосъемниками.

На (рис. 1) приведена физика утечки информации за счет ПЭМИ.

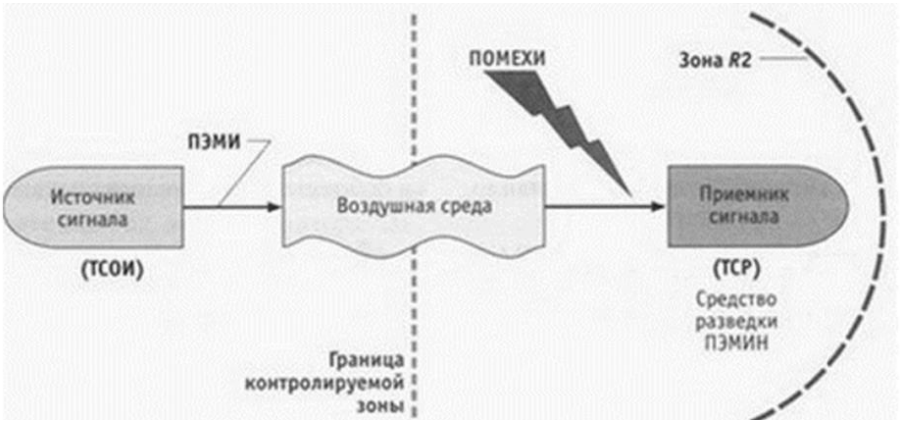


Рисунок 1. Схема ТКУИ за счет ПЭМИ

На (рис. 2) приведена физика утечки информации за счет ПЭМИН.

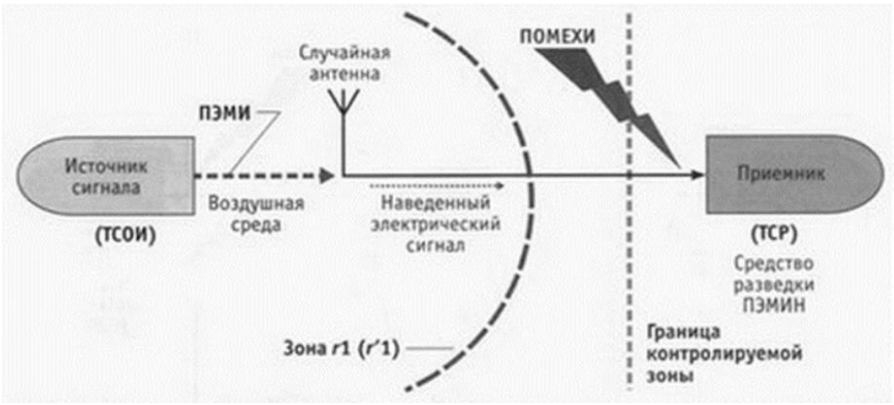


Рисунок 2. Схема ТКУИ за счет ПЭМИН

Поясним некоторые сокращения и термины на схемах:

- ТСОИ – технические средства обработки информации (все что попадает под определение ОТСС);
- ТСР–технические средства разведки;
- зона R2 – расстояние, на котором возможен перехват защищаемой информации за счет ПЭМИ;
- зона r1(r'1) – расстояние, наличие в пределах которого случайных антенн (токоведущие конструкции, линии и ТС) создает возможность утечки информации за счет наводок ПЭМИ.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенной случайной антенной может являться стационарный телефон, датчик пожарной сигнализации, громкоговоритель, подключенная к линии, выходящей за пределы КЗ.

Распределенные случайные антенным – антенны с распределенными параметрами. К ним можно отнести: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ.

Также разделяют саму информации по каналам АЭП и ПЭМИ на случай информативности. Информативные – сигналы с несущей, модулированной информативным сигналом. Примером могут послужить: сигнал от флэш-накопителя USB; VGA-интерфейс монитора; и т.д.

Неинформативные сигналы – сигналы, анализ которых не дает представления об обрабатываемой информации. Примеры: излучения от работы источников питания в узлах ТС; сигнал обработки режимов видеокартой; и т.д.

Важно! Всё приведенное выше относится к составной части по проведению работ, связанных с специальными исследованиями ОТСС и ВТСС. Однако это лишь малая часть того, что можно было бы изложить. Остальная теоретическая и прикладная часть изучается непосредственно работником предприятия в режимно секретном подразделении. Все методические материалы работ, связанных с проведением специальных исследований имеют грифы СЕКРЕТНО и СОВЕРШЕННО СЕКРЕТНО. Вышеизложенный материал является открытым и считается опорным в общих знаниях ТЗИ.

Практическая часть.

Вопросы для самопроверки:

Дайте определение специальным исследованиям в рамках данного учебного занятия.

Какие и сколько существует грифов секретности в рамках законодательства РФ?

Что такое зона r1(r’1) в ТЗИ?

Дайте определение ОТСС и ВТСС и в чем их различие?

На какие категории разбиваются случайные антенны в КЗ и в чем их разница? И на какие категории разбиваются информационные сигналы и в чем их разница?

Практические задания:

Опишите собственными словами следующие определения. ОТСС; ВТСС; ТКУИ.

В соответствии с (рис. 1) данного учебного задания, источником распространения сигнала ПЭМИ между техническим средством и техническим средством разведки является воздушная среда. Что будет если изменить воздушную среду на более плотную, а что, если перенести её в вакуум. Ответ обоснуйте.

Однажды, двое ученых задались очень интересной задачей, связанной с передачей информативного сигнала технического средства через канал ПЭМИ по очень интересной схеме. У них получилось и даже на современном этапе злоумышленники охотно придают значение данному средству получения заведомо важной для них информации. Двух ученых звали Маркус Кун и Росс Андерсон. При помощи сети Интернет, найдите информацию о данной процедуре получения информативного сигнала по каналу ПЭМИ и расскажите в общих чертах об этой технологии

ЗАДАНИЕ № 2

Тема: Теоретические основы средств измерения программно-аппаратных комплексов (ПАК) и альтернативной измерительной площадки (АИП)

Цель работы.

Изучение теоретической основы средств измерений сигналов. Освоить особенности поиска и идентификации сигналов при помощи альтернативной измерительной площадки.

Продолжительность занятия: полтора учебных часа.

Задания.

Изучить теоретическую часть Задания №2.

Выполнить практическую часть Задания №2:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

25. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

В связи с тем, что многие организации, занимающиеся производством и распространением программно-аппаратных комплексов, предлагают на рынке целые линейки своих продуктов, отличающихся только аппаратной частью (анализаторы спектра) и соответственно ценой на данные товары в этой линейке. На рынке представлены программ- но-аппаратные комплексы следующих производителей, распространителей: «Навигатор ПхГ» – «НЕЛК», «Сигурд Мх» – «МАСКОМ», «Легенда» – «АВМ-СИСТЕМС». Стоит отметить, что все комплексы, рассматриваемые в данной работе, имеют сертификаты ФСТЭК России и метрологический сертификат соответствия на измерительное оборудование. Пример ПАК представлен на (рис. 1).

Рисунок 1. ПАК «Сигурд М18»

Требования к антеннам.

В полосе частот от 200 Гц до 30 МГц в комплект антенн должны входить магнитная и (или) электрическая антенны.

Для измерения магнитной составляющей электромагнитного поля, антенна должна быть: электрически экранированной рамочной антенной, имеющей такие размеры, чтобы ее рамка помещалась в квадрат со стороной не более 0,6 м, или ферритовая антенна длиной не более 0,5 м.

Допускаемая погрешность измерений напряженности магнитного поля (измеритель с магнитной антенной) не должна превышать 2,5 дБ.

Конструкция антенн (антенного штатива) должна обеспечивать возможность плавного изменения высоты расположения антенны над землей от 0,8 м до 1,25 м, а также возможность поворота магнитной и электрической антенн на 360° вокруг оси.

В полосе частот от 30 до 1000 МГц в комплект антенн должны входить одна или несколько электрических антенн одного из следующих типов:

а) линейный симметричный вибратор на полосу частот от 30 до 80 МГц, размер которого равен длине полуволнового симметричного вибратора на частоте 80 МГц, и настраиваемый полуволновой симметричный вибратор в полосе частот от 80 до 1000 МГц, имеющий КСВН не более 2,5;

б) биконическая антенна, максимальный размер которой должен быть не более 1,35 м в полосе частот от 30 до 300 МГц и с КСВН не более 3,0, и биконическая антенна, максимальный размер которой – не более 0,5 м в полосе частот от 300 до 1000 МГц с КСВН не более 2,5;

в) широкополосная антенна, главный лепесток диаграммы направленности которой должен быть таким, чтобы в направлении непосредственного излучения от источника ПЭМИН и в направлении отраженного от земли луча разность коэффициентов усиления антенны не превышала бы 1 дБ, с КСВН не более 2,5.

Конструкция антенны (антенного штатива) должна обеспечивать возможность плавного изменения высоты центра симметрии над землей от 1 до

4 м и поворота вокруг горизонтальной оси на 180°, а также фиксированную ориентацию в трех взаимно ортогональных направлениях.

Допускаемая погрешность измерений напряженности электрического поля (измеритель с биконической, электрической антенной) не должна превышать 2,5 дБ на частотах до 1000 МГц.

Антенны должны иметь коэффициент калибровки, позволяющий измерять уровни полей. Рекомендуемый коэффициент калибровки антенн – не более 40 дБ. Погрешность коэффициента калибровки антенн должна быть не более 2 дБ.

Требования к анализатору.

Должен иметь несимметричный вход с номинальным значением сопротивления 50 Ом с коэффициентом стоячей волны по напряжению (КСВН) не более 2 при ослаблении входного аттенюатора 0 дБ и не более 1,2 при ослаблении входного аттенюатора 10 дБ и более.

Измерители совместно с первичными преобразователями должны обеспечивать измерения характеристик ПЭМИ в децибелах, относительно 1 мкВ, 1 мкА, 1 мкВ/м, 1 мкА/м, 1 мВт/м2.

Анализатор спектра должен быть программируемым, для дистанционного управления, т. е. должен обрабатывать команды, которые ему посылает ПЭВМ.

Должен иметь интерфейсы LAN или USB, или GPIB, или RS-232 для передачи данных с ПЭВМ на анализатор спектра и обратно.

Анализатор спектра должен иметь квазипиковый, пиковый и со среднеквадратичным отклонением детекторы.

Работать в полосе частот 9 кГц...1000 МГц.

Иметь полосы пропускания в диапазоне 1 кГц...3 МГц. Погрешность, вносимая собственными шумами, должна быть не более 1 дБ. Анализатор спектра должен обеспечивать звуковой контроль ПЭМИ, имеющих амплитудную и частотную (на частотах свыше 30 МГц) модуляцию, с помощью встроенных или подключаемых приборов или устройств.

Примерный перечень оборудования приведен в (табл. 1).

Таблица 1. Перечень оборудования для проведения оценки защищенности по каналу ПЭМИН

Наименование средств измерения	Тип	Диапазон частот
Анализатор спектра	LIGNext1 NS-30A	10 кГц -3 ГГц
Антенна магнитная рамочная активная	Н-30	10 Гц – 30 МГц
Антенна электрическая дипольная активная	Е-3000	30 МГц – 3000 МГц
Антенна электрическая дипольная активная	Е-30	10 Гц – 30 МГц
Пробник напряжения	П-400	10 Гц – 300 МГц
Осциллограф	LeCroy Wavesurfer 62Xs	0 Гц – 600 МГц
Генератор сигналов	Г4-218	200 кГц-1 ГГц

Альтернативная измерительная площадка.

Временная методика оценки защищенности ОТСС, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации (КИ), описанная в «Сборнике временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам» предполагает собой поиск и измерение опасных сигналов непосредственно на объекте информатизации.

Однако, шумовая обстановка на объекте информатизации весьма нестабильна. Помимо нестабильности она абсолютно неисследованная. Оператор при проведении измерений может столкнуться с таким явлением как «стоячая волна».

Стоячая волна (электромагнитная) – периодическое изменение амплитуды напряженности электрического и магнитного полей вдоль направления

распространения, вызванное интерференцией, падающей и отраженной волн. Например, стоячая волна возникает при отражении волны от преград и неоднородностей в результате взаимодействия (интерференции), падающей и отражённой волн.

Присутствие такой волны во время проведения измерений однозначно приведёт к ошибке.

Измерительная площадка – площадка, отвечающая требованиям, обеспечивающим правильное измерение уровней индустриальных радиопомех (ИРП), излучаемых ТС в регламентированных условиях. Видов ИП предусматриваются два – «открытая измерительная площадка» и «альтернативная измерительная площадка». Поскольку строительство и эксплуатация открытой площадки весьма дорого, сосредоточимся на более дешёвом варианте – АИП. Разница между открытой ИП и АИП заключается в том, что последняя должна размещаться не в открытом пространстве, а в некотором помещении, в здании. При том физические характеристики АИП (прежде всего «затухание» электромагнитного поля) должны оставаться в пределах установленного допуска.

Важно! Перед вводом в эксплуатацию АИП оценивается минимум искажений, вносимых в распределение электромагнитного поля ограждающими конструкциями помещения, который можно допустить. Иными словами, оператор заранее знает о наличии и характере «стоячих волн» и о характеристиках закона затухания электромагнитного поля. Это позволяет получать информацию об «опасных» информативных сигналах корректнее, чем на ОИ, на котором абсолютно не исследована шумовая обстановка.

Практическая часть.

Вопросы для самопроверки:

Назовите весь перечень оборудования для проведения оценки защищенности по ПЭМИ.

Дайте определение измерительной площадки в рамках данного задания.

Сколько существует видов измерительных площадок (ИП) и в чем их различие?

На сколько метров минимально и максимально предполагается плавное размещение антенны по высоте?

Какой должен быть коэффициент калибровки у антенн?

Практические задания:

Как по Вашему мнению вы представляете себе открытую измерительную площадку и альтернативную? Опишите их. В чем их основное различие? Ответ обоснуйте.

Представьте, что Вы начинающий сотрудник предприятия ООО «НПП «ИБЦ». Начался ваш седьмой рабочий день. Вы в обычном распорядке, получив задание, идете включать лабораторное автоматизированное рабочее место и ПАК. Неожиданным образом узнаёте, что откалиброванная антенна начала давать сбой. Вы (без особой паники) начинаете искать пути решения. По Вашему мнению, каковы основные три шага на пути решения этой проблемы? Ответ обоснуйте.

Лабораторная работа № 4.
Тема: Основные положения формальной теории защиты информации
Цель занятия: Концепция монитора безопасности обращений в КС.
Правила разграничения доступа субъектов к объектам в ОС.
Монитор безопасности обращений (МБО) субъектов к объектам. Схема монитора безопасности обращений. Функции МБО. Свойства МБО
Продолжительность практического занятия-0.5 часа
Задание.

ЗАДАНИЕ № 1

Тема: Теоретические аспекты проведения специальных исследований (СИ) на предприятии

Цель работы.

Изучение основных принципов проведения специальных исследований на предприятии. Освоить структуру ведения общей теоретической части проведения специальных исследований.

Продолжительность занятия: полтора учебных часа.

Задания.

Изучить теоретическую часть Задания №1.

Выполнить практическую часть Задания №1:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

26. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Специальные исследования (специсследования, СИ) — комплекс действий, направленный на обнаружение потенциальных технических каналов утечки защищаемой информации с помощью специального контрольно-измерительного оборудования, в соответствии с нормативно-методическими документами ФСБ России и ФСТЭК России.

Проведение специсследований определяет возможность считывания и перехвата сигнала специальными средствами разведки в рамках определённых границ (защищённость утечек по каналам ПЭМИН — побочные электромагнитные излучения и наводки).

Введем для большей ясности определения, связанные с основой ведения специсследований на предприятии. Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается ценная информация.

Автоматизированная система (АС) – устройство или комплекс устройств, необходимых для передачи, хранения и обработки конфиденци-

альной информации, прошедшая процедуру аттестации в соответствии с законодательством РФ.

Контролируемая зона (КЗ) – пространство, в котором исключено неконтролируемое пребывание посторонних лиц или сотрудников, не имеющих прямое отношение к данному пространству. Примерами могут послужить: периметр охраняемой территории; ограждающие конструкции охраняемого здания или охраняемой территории.

Информационный сигнал – электрические сигналы, акустические, электромагнитные и т.д., по параметрам которых можно раскрыть конфиденциальную информацию, передаваемую, хранимую или обрабатываемую в основных технических средствах и системах или обсуждаемая в защищенном исполнении.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для обработки, хранения и передачи конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

Средства активной защиты информации по каналам ПЭМИН (САЗ) – технические средства формирования маскирующих электромагнитных помех в местах возможного съема защищаемой информации, прошедшие обязательную процедуру сертификации по линии ФСТЭК России.

Деятельность по технической защите конфиденциальной информации (ТЗКИ) – выполнение работ и (или) оказание услуг по ее защите:

– от несанкционированного доступа,

– от утечки по техническим каналам,

– от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Важно! Данный вид деятельности является лицензируемым. Лицензирование деятельности по ТЗКИ осуществляет ФСТЭК России.

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные поля, создаваемые в окружающем пространстве СВТ, специально для этого не предназначенными (в случае ПЭМИ) или наводки данных излучений на токоведущие конструкции, линии и подключенные к ним ТС.

Существует несколько видов проведения специсследований на определенные ТС. В данном случае это акустоэлектрическое преобразование (АЭП) и ПЭМИН. В случае АЭП исследуемое средство подвергается воздействию некоих акустических частот. Из этого обосновывается определенный вывод о возможности использования ТС на невозможности подверженности АЭП.

Как уже было указано в определениях, ПЭМИ создаются вокруг работающих технических средств, которые специально для данного излучения не создавались. То есть излучение от радиопередатчиков, мобильных телефонов – это не побочные излучения. А вот излучения при работе компьютера от монитора, принтера, накопителей информации являются побочными.

Если вспомнить физику, то вокруг проводника, по которому протекает электрический ток возникает электромагнитное поле. Если по данному проводнику передается какой-либо сигнал, то, следовательно, и электромагнитное поле тоже будет изменяться по тем же законам, что и сигнал, протекающий в линии. Таким образом, источником сигнала ПЭМИ являются все токоведущие линии в ТС, по которым в процессе работы передаются какие-либо сигналы.

Как известно электромагнитные поля могут распространяться на значительные расстояния и конструкции помещений тому не преграда. Скорость передачи данных и обработки информации в современных средствах вычислительной техники постоянно растет, а значит растут и частоты сигналов ПЭМИ. Частоты сигналов ПЭМИ могут начинаться от единиц кГц и заканчиваться единицами ГГц, а гармоники этих сигналов могут находиться еще выше по частоте.

Если вспомнить, что в проводнике, помещенном в электромагнитное поле, возникает электрический ток, то очевидно, что могут возникать наводки ПЭМИ на любые токоведущие элементы (систему отопления, короб системы вентиляции и т. д.), в том числе и любые линии и ТС, подключенные к ним, попадающие под действие данного электромагнитного поля.

Перехват этой информации можно осуществить путем анализа изменений параметров ПЭМИН с помощью специальных высокочувствительных радиоприемных устройств, оснащенных специализированными антеннами, пробниками напряжения, токосъемниками.

На (рис. 1) приведена физика утечки информации за счет ПЭМИ.

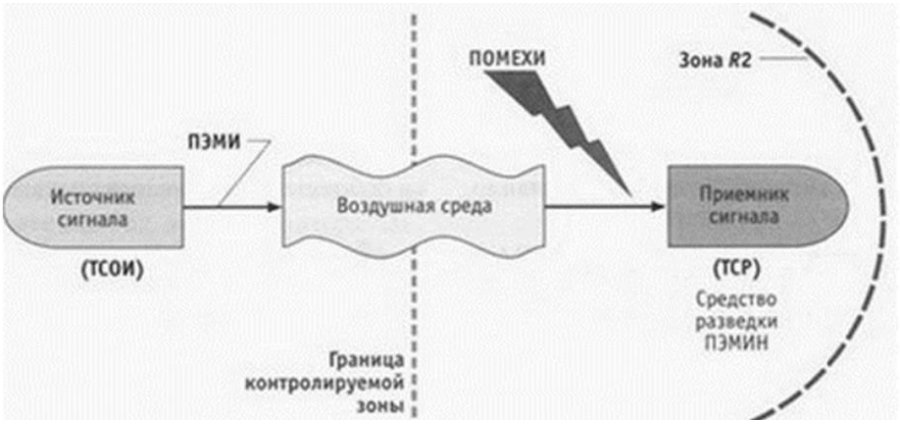


Рисунок 1. Схема ТКУИ за счет ПЭМИ

На (рис. 2) приведена физика утечки информации за счет ПЭМИН.

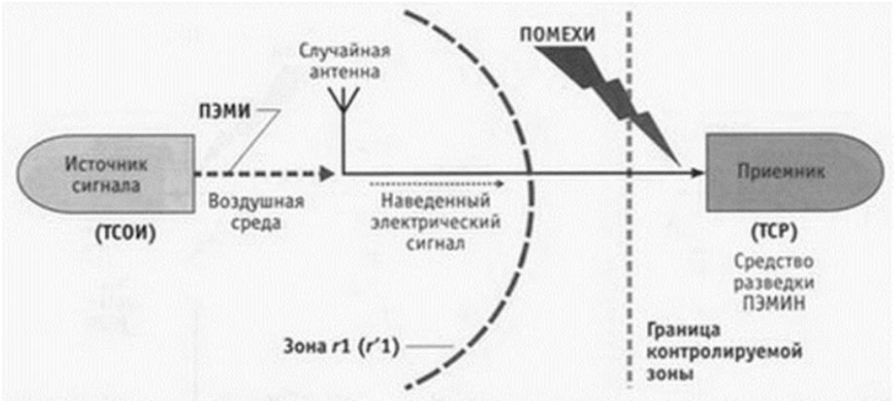


Рисунок 2. Схема ТКУИ за счет ПЭМИН

Поясним некоторые сокращения и термины на схемах:

• ТСОИ – технические средства обработки информации (все что попадает под определение ОТСС);

• ТСР–технические средства разведки;

• зона R2 – расстояние, на котором возможен перехват защищаемой информации за счет ПЭМИ;

• зона r1(r’1) – расстояние, наличие в пределах которого случайных антенн (токоведущие конструкции, линии и ТС) создает возможность утечки информации за счет наводок ПЭМИ.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенной случайной антенной может являться стационарный телефон, датчик пожарной сигнализации, громкоговоритель, подключенная к линии, выходящей за пределы КЗ.

Распределенные случайные антенным – антенны с распределенными параметрами. К ним можно отнести: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ.

Также разделяют саму информации по каналам АЭП и ПЭМИ на случай информативности. Информативные – сигналы с несущей, модулированной информативным сигналом. Примером могут послужить: сигнал от флэш-накопителя USB; VGA-интерфейс монитора; и т.д.

Неинформативные сигналы – сигналы, анализ которых не дает представления об обрабатываемой информации. Примеры: излучения от работы источников питания в узлах ТС; сигнал обработки режимов видеокартой; и т.д.

Важно! Всё приведенное выше относится к составной части по проведению работ, связанных с специальными исследованиями ОТСС и ВТСС. Однако это лишь малая часть того, что можно было бы изложить. Остальная теоретическая и прикладная часть изучается непосредственно работником предприятия в режимно секретном подразделении. Все методические материалы работ, связанных с проведением специальных исследований имеют грифы СЕКРЕТНО и СОВЕРШЕННО СЕКРЕТНО. Вышеизложенный материал является открытым и считается опорным в общих знаниях ТЗИ.

Практическая часть.

Вопросы для самопроверки:

Дайте определение специальным исследованиям в рамках данного учебного занятия.

Какие и сколько существует грифов секретности в рамках законодательства РФ?

Что такое зона r1(r'1) в ТЗИ?

Дайте определение ОТСС и ВТСС и в чем их различие?

На какие категории разбиваются случайные антенны в КЗ и в чем их разница? И на какие категории разбиваются информационные сигналы и в чем их разница?

Практические задания:

Опишите собственными словами следующие определения. ОТСС; ВТСС; ТКУИ.

В соответствии с (рис. 1) данного учебного задания, источником распространения сигнала ПЭМИ между техническим средством и техническим средством разведки является воздушная среда. Что будет если изменить воздушную среду на более плотную, а что, если перенести её в вакуум. Ответ обоснуйте.

Однажды, двое ученых задались очень интересной задачей, связанной с передачей информативного сигнала технического средства через канал ПЭМИ по очень интересной схеме. У них получилось и даже на современном этапе злоумышленники охотно придают значение данному средству получения заведомо важной для них информации. Двух ученых звали Маркус Кун и Росс Андерсон. При помощи сети Интернет, найдите информацию о данной процедуре получения информативного сигнала по каналу ПЭМИ и расскажите в общих чертах об этой технологии

ЗАДАНИЕ № 2

Тема: Теоретические основы средств измерения программно-аппаратных комплексов (ПАК) и альтернативной измерительной площадки (АИП)

Цель работы.

Изучение теоретической основы средств измерений сигналов. Освоить особенности поиска и идентификации сигналов при помощи альтернативной измерительной площадки.

Продолжительность занятия: полтора учебных часа.

Задания.

Изучить теоретическую часть Задания №2.

Выполнить практическую часть Задания №2:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

В связи с тем, что многие организации, занимающиеся производством и распространением программно-аппаратных комплексов, предлагают на рынке целые линейки своих продуктов, отличающихся только аппаратной частью (анализаторы спектра) и соответственно ценой на данные товары в этой линейке. На рынке представлены программ- но-аппаратные комплексы следующих производителей, распространителей: «Навигатор ПхГ» – «НЕЛК», «Сигурд Мх» – «МАСКОМ», «Легенда» – «АВМ-СИСТЕМС». Стоит отметить, что все комплексы, рассматриваемые в данной работе, имеют сертификаты ФСТЭК России и метрологический сертификат соответствия на измерительное оборудование. Пример ПАК представлен на (рис. 1).

Рисунок 1. ПАК «Сигурд М18»

Требования к антеннам.

В полосе частот от 200 Гц до 30 МГц в комплект антенн должны входить магнитная и (или) электрическая антенны.

Для измерения магнитной составляющей электромагнитного поля, антенна должна быть: электрически экранированной рамочной антенной, имеющей такие размеры, чтобы ее рамка помещалась в квадрат со стороной не более 0,6 м, или ферритовая антенна длиной не более 0,5 м.

Допускаемая погрешность измерений напряженности магнитного поля (измеритель с магнитной антенной) не должна превышать 2,5 дБ.

Конструкция антенн (антенного штатива) должна обеспечивать возможность плавного изменения высоты расположения антенны над землей от 0,8 м до 1,25 м, а также возможность поворота магнитной и электрической антенн на 360° вокруг оси.

В полосе частот от 30 до 1000 МГц в комплект антенн должны входить одна или несколько электрических антенн одного из следующих типов:

а) линейный симметричный вибратор на полосу частот от 30 до 80 МГц, размер которого равен длине полуволнового симметричного вибратора

на частоте 80 МГц, и настраиваемый полуволновой симметричный вибратор в полосе частот от 80 до 1000 МГц, имеющий КСВН не более 2,5;

б) биконическая антенна, максимальный размер которой должен быть не более 1,35 м в полосе частот от 30 до 300 МГц и с КСВН не более 3,0, и биконическая антенна, максимальный размер которой – не более 0,5 м в полосе частот от 300 до 1000 МГц с КСВН не более 2,5;

в) широкополосная антенна, главный лепесток диаграммы направленности которой должен быть таким, чтобы в направлении непосредственного излучения от источника ПЭМИН и в направлении отраженного от земли луча разность коэффициентов усиления антенны не превышала бы 1 дБ, с КСВН не более 2,5.

Конструкция антенны (антенного штатива) должна обеспечивать возможность плавного изменения высоты центра симметрии над землей от 1 до 4 м и поворота вокруг горизонтальной оси на 180°, а также фиксированную ориентацию в трех взаимно ортогональных направлениях.

Допускаемая погрешность измерений напряженности электрического поля (измеритель с биконической, электрической антенной) не должна превышать 2,5 дБ на частотах до 1000 МГц.

Антенны должны иметь коэффициент калибровки, позволяющий измерять уровни полей. Рекомендуемый коэффициент калибровки антенн – не более 40 дБ. Погрешность коэффициента калибровки антенн должна быть не более 2 дБ.

Требования к анализатору.

Должен иметь несимметричный вход с номинальным значением сопротивления 50 Ом с коэффициентом стоячей волны по напряжению (КСВН) не более 2 при ослаблении входного аттенюатора 0 дБ и не более 1,2 при ослаблении входного аттенюатора 10 дБ и более.

Измерители совместно с первичными преобразователями должны обеспечивать измерения характеристик ПЭМИ в децибелах, относительно 1 мкВ, 1 мкА, 1 мкВ/м, 1 мкА/м, 1 мВт/м2.

Анализатор спектра должен быть программируемым, для дистанционного управления, т. е. должен обрабатывать команды, которые ему посылает ПЭВМ.

Должен иметь интерфейсы LAN или USB, или GPIB, или RS-232 для передачи данных с ПЭВМ на анализатор спектра и обратно.

Анализатор спектра должен иметь квазипиковый, пиковый и со среднеквадратичным отклонением детекторы.

Работать в полосе частот 9 кГц...1000 МГц.

Иметь полосы пропускания в диапазоне 1 кГц...3 МГц. Погрешность, вносимая собственными шумами, должна быть не более 1 дБ. Анализатор спектра должен обеспечивать звуковой контроль ПЭМИ, имеющих амплитудную и частотную (на частотах свыше 30 МГц) модуляцию, с помощью встроенных или подключаемых приборов или устройств.

Примерный перечень оборудования приведен в (табл. 1).

Таблица 1. Перечень оборудования для проведения оценки защищенности по каналу ПЭМИН

Наименование средств измерения	Тип	Диапазон частот
Анализатор спектра	LIGNext1 NS-30A	10 кГц -3 ГГц
Антенна магнитная рамочная активная	Н-30	10 Гц – 30 МГц
Антенна электрическая дипольная активная	Е-3000	30 МГц – 3000 МГц
Антенна электрическая дипольная активная	Е-30	10 Гц – 30 МГц
Пробник напряжения	П-400	10 Гц – 300 МГц
Осциллограф	LeCroy Wavesurfer 62Xs	0 Гц – 600 МГц
Генератор сигналов	Г4-218	200 кГц-1 ГГц

Альтернативная измерительная площадка.

Временная методика оценки защищенности ОТСС, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации (КИ), описанная в «Сборнике временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам» предполагает собой поиск и измерение опасных сигналов непосредственно на объекте информатизации.

Однако, шумовая обстановка на объекте информатизации весьма нестабильна. Помимо нестабильности она абсолютно неисследованная. Оператор при проведении измерений может столкнуться с таким явлением как «стоячая волна».

Стоячая волна (электромагнитная) – периодическое изменение амплитуды напряженности электрического и магнитного полей вдоль направления распространения, вызванное интерференцией, падающей и отраженной волн. Например, стоячая волна возникает при отражении волны от преград и неоднородностей в результате взаимодействия (интерференции), падающей и отражённой волн.

Присутствие такой волны во время проведения измерений однозначно приведёт к ошибке.

Измерительная площадка – площадка, отвечающая требованиям, обеспечивающим правильное измерение уровней индустриальных радиопомех (ИРП), излучаемых ТС в регламентированных условиях. Видов ИП предусматриваются два – «открытая измерительная площадка» и «альтернативная измерительная площадка». Поскольку строительство и эксплуатация открытой площадки весьма дорого, сосредоточимся на более дешёвом варианте – АИП. Разница между открытой ИП и АИП заключается в том, что последняя должна размещаться не в открытом пространстве, а в некотором помещении, в здании. При том физические характеристики АИП (прежде всего «затухание» электромагнитного поля) должны оставаться в пределах установленного допуска.

Важно! Перед вводом в эксплуатацию АИП оценивается минимум искажений, вносимых в распределение электромагнитного поля ограждающими конструкциями помещения, который можно допустить. Иными словами, оператор заранее знает о наличии и характере «стоячих волн» и о характеристиках закона затухания электромагнитного поля. Это позволяет получать информацию об «опасных» информативных сигналах корректнее, чем на ОИ, на котором абсолютно не исследована шумовая обстановка.

Практическая часть.

Вопросы для самопроверки:

Назовите весь перечень оборудования для проведения оценки защищенности по ПЭМИ.

Дайте определение измерительной площадки в рамках данного задания.

Сколько существует видов измерительных площадок (ИП) и в чем их различие?

На сколько метров минимально и максимально предполагается плавное размещение антенны по высоте?

Какой должен быть коэффициент калибровки у антенн?

Практические задания:

Как по Вашему мнению вы представляете себе открытую измерительную площадку и альтернативную? Опишите их. В чем их основное различие? Ответ обоснуйте.

Представьте, что Вы начинающий сотрудник предприятия ООО «НПП «ИБЦ». Начался ваш седьмой рабочий день. Вы в обычном распорядке, получив задание, идете включать лабораторное автоматизированное рабочее место и ПАК. Неожиданным образом узнаёте, что откалиброванная антенна начала давать сбой. Вы (без особой паники)

начинаете искать пути решения. По Вашему мнению, каковы основные три шага на пути решения этой проблемы? Ответ обоснуйте.

Лабораторная работа № 5.
Тема: Формальные модели безопасности
Цель занятия: Общий подход к построению систем, реализующих мандатную (полномочную) политику безопасности в модели BL (Белла-Лападулы).
Назначение модели Белла-Лападулы. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы.
Условие определения безопасности системы. Свойства безопасности системы. Проверка безопасности системы. Основные теоремы и определения состояний системы.
Эквивалентные подходы к определению безопасности модели Белла-Лападулы. Недостатки модели Белла-Лападулы.
Продолжительность практического занятия-1 часа
Задание.

ЗАДАНИЕ № 1

Тема: Теоретические аспекты проведения специальных исследований (СИ) на предприятии

Цель работы.

Изучение основных принципов проведения специальных исследований на предприятии. Освоить структуру ведения общей теоретической части проведения специальных исследований.

Продолжительность занятия: полтора учебных часа.

Задания.

Изучить теоретическую часть Задания №1.

Выполнить практическую часть Задания №1:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Специальные исследования (специсследования, СИ) — комплекс действий, направленный на обнаружение потенциальных технических каналов

утечки защищаемой информации с помощью специального контрольно-измерительного оборудования, в соответствии с нормативно-методическими документами ФСБ России и ФСТЭК России.

Проведение специсследований определяет возможность считывания и перехвата сигнала специальными средствами разведки в рамках определённых границ (защищённость утечек по каналам ПЭМИН — побочные электромагнитные излучения и наводки).

Введем для большей ясности определения, связанные с основой ведения специсследований на предприятии. Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается ценная информация.

Автоматизированная система (АС) – устройство или комплекс устройств, необходимых для передачи, хранения и обработки конфиденциальной информации, прошедшая процедуру аттестации в соответствии с законодательством РФ.

Контролируемая зона (КЗ) – пространство, в котором исключено неконтролируемое пребывание посторонних лиц или сотрудников, не имеющих прямое отношение к данному пространству. Примерами могут послужить: периметр охраняемой территории; ограждающие конструкции охраняемого здания или охраняемой территории.

Информационный сигнал – электрические сигналы, акустические, электромагнитные и т.д., по параметрам которых можно раскрыть конфиденциальную информацию, передаваемую, хранимую или обрабатываемую в основных технических средствах и системах или обсуждаемая в защищенном исполнении.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для обработки, хранения и передачи конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

Средства активной защиты информации по каналам ПЭМИН (САЗ) – технические средства формирования маскирующих электромагнитных помех в местах возможного съема защищаемой информации, прошедшие обязательную процедуру сертификации по линии ФСТЭК России.

Деятельность по технической защите конфиденциальной информации (ТЗКИ) – выполнение работ и (или) оказание услуг по ее защите:

– от несанкционированного доступа,

– от утечки по техническим каналам,

– от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Важно! Данный вид деятельности является лицензируемым. Лицензирование деятельности по ТЗКИ осуществляет ФСТЭК России.

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные поля, создаваемые в окружающем пространстве СВТ, специально для этого не предназначенными (в случае ПЭМИ) или наводки данных излучений на токоведущие конструкции, линии и подключенные к ним ТС.

Существует несколько видов проведения специсследований на определенные ТС. В данном случае это акустоэлектрическое преобразование (АЭП) и ПЭМИН. В случае АЭП исследуемое средство подвергается воздействию некоих акустических частот. Из этого обосновывается определенный вывод о возможности использования ТС на невозможности подверженности АЭП.

Как уже было указано в определениях, ПЭМИ создаются вокруг работающих технических средств, которые специально для данного излучения не создавались. То есть излучение от радиопередатчиков, мобильных телефонов

– это не побочные излучения. А вот излучения при работе компьютера от монитора, принтера, накопителей информации являются побочными.

Если вспомнить физику, то вокруг проводника, по которому протекает электрический ток возникает электромагнитное поле. Если по данному проводнику передается какой-либо сигнал, то, следовательно, и электромагнитное поле тоже будет изменяться по тем же законам, что и сигнал, протекающий в линии. Таким образом, источником сигнала ПЭМИ являются все токоведущие линии в ТС, по которым в процессе работы передаются какие-либо сигналы.

Как известно электромагнитные поля могут распространяться на значительные расстояния и конструкции помещений тому не преграда. Скорость передачи данных и обработки информации в современных средствах вычислительной техники постоянно растет, а значит растут и частоты сигналов ПЭМИ. Частоты сигналов ПЭМИ могут начинаться от единиц кГц и заканчиваться единицами ГГц, а гармоники этих сигналов могут находиться еще выше по частоте.

Если вспомнить, что в проводнике, помещенном в электромагнитное поле, возникает электрический ток, то очевидно, что могут возникать наводки ПЭМИ на любые токоведущие элементы (систему отопления, короб системы вентиляции и т. д.), в том числе и любые линии и ТС, подключенные к ним, попадающие под действие данного электромагнитного поля.

Перехват этой информации можно осуществить путем анализа изменений параметров ПЭМИН с помощью специальных высокочувствительных радиоприемных устройств, оснащенных специализированными антеннами, пробниками напряжения, токосъемниками.

На (рис. 1) приведена физика утечки информации за счет ПЭМИ.

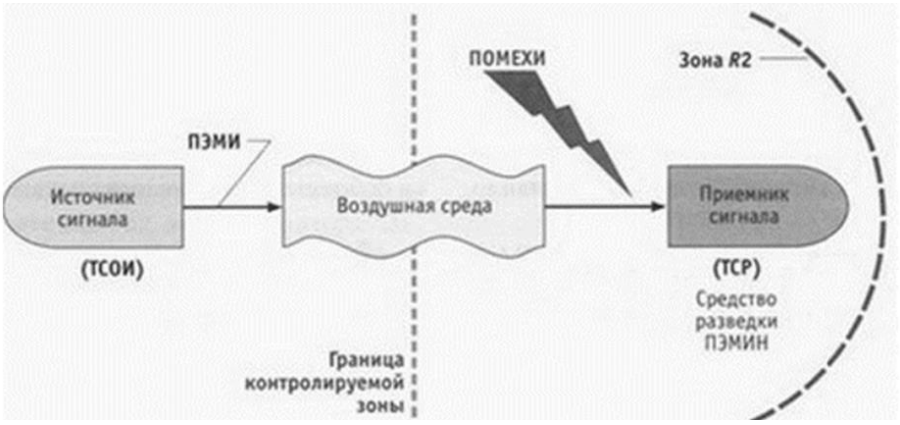


Рисунок 1. Схема ТКУИ за счет ПЭМИ

На (рис. 2) приведена физика утечки информации за счет ПЭМИН.

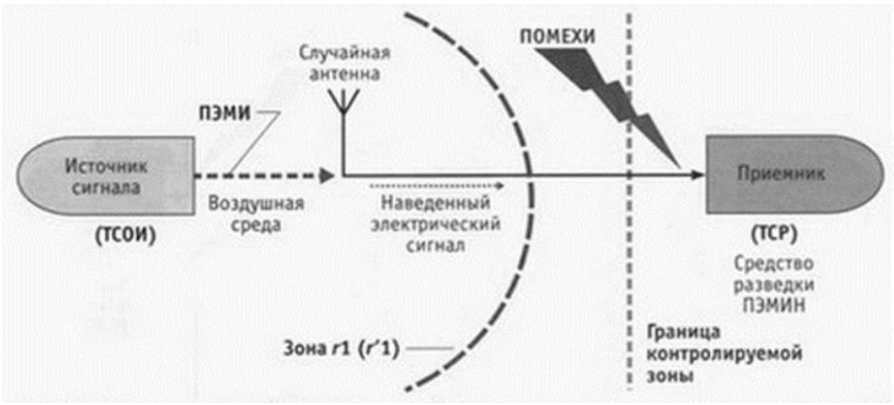


Рисунок 2. Схема ТКУИ за счет ПЭМИН

Поясним некоторые сокращения и термины на схемах:

- ТСОИ – технические средства обработки информации (все что попадает под определение ОТСС);
- ТСР–технические средства разведки;
- зона R2 – расстояние, на котором возможен перехват защищаемой информации за счет ПЭМИ;
- зона r1(r'1) – расстояние, наличие в пределах которого случайных антенн (токоведущие конструкции, линии и ТС) создает возможность утечки информации за счет наводок ПЭМИ.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенной случайной антенной может являться стационарный телефон, датчик пожарной сигнализации, громкоговоритель, подключенная к линии, выходящей за пределы КЗ.

Распределенные случайные антенным – антенны с распределенными параметрами. К ним можно отнести: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ.

Также разделяют саму информации по каналам АЭП и ПЭМИ на случай информативности. Информативные – сигналы с несущей, модулированной информативным сигналом. Примером могут послужить: сигнал от флэш-накопителя USB; VGA-интерфейс монитора; и т.д.

Неинформативные сигналы – сигналы, анализ которых не дает представления об обрабатываемой информации. Примеры: излучения от работы источников питания в узлах ТС; сигнал обработки режимов видеокартой; и т.д.

Важно! Всё приведенное выше относится к составной части по проведению работ, связанных с специальными исследованиями ОТСС и ВТСС. Однако это лишь малая часть того, что можно было бы изложить. Остальная теоретическая и прикладная часть изучается непосредственно работником предприятия в режимно секретном подразделении. Все методические материалы работ, связанных с проведением специальных исследований имеют грифы СЕКРЕТНО и СОВЕРШЕННО СЕКРЕТНО. Вышеизложенный материал является открытым и считается опорным в общих знаниях ТЗИ.

Практическая часть.

Вопросы для самопроверки:

Дайте определение специальным исследованиям в рамках данного учебного занятия.

Какие и сколько существует грифов секретности в рамках законодательства РФ?

Что такое зона r1(r’1) в ТЗИ?

Дайте определение ОТСС и ВТСС и в чем их различие?

На какие категории разбиваются случайные антенны в КЗ и в чем их разница? И на какие категории разбиваются информационные сигналы и в чем их разница?

Практические задания:

Опишите собственными словами следующие определения. ОТСС; ВТСС; ТКУИ.

В соответствии с (рис. 1) данного учебного задания, источником распространения сигнала ПЭМИ между техническим средством и техническим средством разведки является воздушная среда. Что будет если изменить воздушную среду на более плотную, а что, если перенести её в вакуум. Ответ обоснуйте.

Однажды, двое ученых задались очень интересной задачей, связанной с передачей информативного сигнала технического средства через канал ПЭМИ по очень интересной схеме. У них получилось и даже на современном этапе злоумышленники охотно придают значение данному средству получения заведомо важной для них информации. Двух ученых звали Маркус Кун и Росс Андерсон. При помощи сети Интернет, найдите информацию о данной процедуре получения информативного сигнала по каналу ПЭМИ и расскажите в общих чертах об этой технологии

ЗАДАНИЕ № 2

Тема: Теоретические основы средств измерения программно-аппаратных комплексов (ПАК) и альтернативной измерительной площадки (АИП)

Цель работы.

Изучение теоретической основы средств измерений сигналов. Освоить особенности поиска и идентификации сигналов при помощи альтернативной измерительной площадки.

Продолжительность занятия: полтора учебных часа.

Задания.

Изучить теоретическую часть Задания №2.

Выполнить практическую часть Задания №2:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

В связи с тем, что многие организации, занимающиеся производством и распространением программно-аппаратных комплексов, предлагают на рынке целые линейки своих продуктов, отличающихся только аппаратной частью (анализаторы спектра) и соответственно ценой на данные товары в этой линейке. На рынке представлены программ- но-аппаратные комплексы следующих производителей, распространителей: «Навигатор ПхГ» – «НЕЛК», «Сигурд Мх» – «МАСКОМ», «Легенда» – «АВМ-СИСТЕМС». Стоит отметить, что все комплексы, рассматриваемые в данной работе, имеют сертификаты ФСТЭК России и метрологический сертификат соответствия на измерительное оборудование. Пример ПАК представлен на (рис. 1).

Рисунок 1. ПАК «Сигурд М18»

Требования к антеннам.

В полосе частот от 200 Гц до 30 МГц в комплект антенн должны входить магнитная и (или) электрическая антенны.

Для измерения магнитной составляющей электромагнитного поля, антенна должна быть: электрически экранированной рамочной антенной, имеющей такие размеры, чтобы ее рамка помещалась в квадрат со стороной не более 0,6 м, или ферритовая антенна длиной не более 0,5 м.

Допускаемая погрешность измерений напряженности магнитного поля (измеритель с магнитной антенной) не должна превышать 2,5 дБ.

Конструкция антенн (антенного штатива) должна обеспечивать возможность плавного изменения высоты расположения антенны над землей от 0,8 м до 1,25 м, а также возможность поворота магнитной и электрической антенн на 360° вокруг оси.

В полосе частот от 30 до 1000 МГц в комплект антенн должны входить одна или несколько электрических антенн одного из следующих типов:

а) линейный симметричный вибратор на полосу частот от 30 до 80 МГц, размер которого равен длине полуволнового симметричного вибратора на частоте 80 МГц, и настраиваемый полуволновой симметричный вибратор в полосе частот от 80 до 1000 МГц, имеющий КСВН не более 2,5;

б) биконическая антенна, максимальный размер которой должен быть не более 1,35 м в полосе частот от 30 до 300 МГц и с КСВН не более 3,0, и биконическая антенна, максимальный размер которой – не более 0,5 м в полосе частот от 300 до 1000 МГц с КСВН не более 2,5;

в) широкополосная антенна, главный лепесток диаграммы направленности которой должен быть таким, чтобы в направлении непосредственного излучения от источника ПЭМИН и в направлении отраженного от земли луча разность коэффициентов усиления антенны не превышала бы 1 дБ, с КСВН не более 2,5.

Конструкция антенны (антенного штатива) должна обеспечивать возможность плавного изменения высоты центра симметрии над землей от 1 до

4 м и поворота вокруг горизонтальной оси на 180°, а также фиксированную ориентацию в трех взаимно ортогональных направлениях.

Допускаемая погрешность измерений напряженности электрического поля (измеритель с биконической, электрической антенной) не должна превышать 2,5 дБ на частотах до 1000 МГц.

Антенны должны иметь коэффициент калибровки, позволяющий измерять уровни полей. Рекомендуемый коэффициент калибровки антенн – не более 40 дБ. Погрешность коэффициента калибровки антенн должна быть не более 2 дБ.

Требования к анализатору.

Должен иметь несимметричный вход с номинальным значением сопротивления 50 Ом с коэффициентом стоячей волны по напряжению (КСВН) не более 2 при ослаблении входного аттенюатора 0 дБ и не более 1,2 при ослаблении входного аттенюатора 10 дБ и более.

Измерители совместно с первичными преобразователями должны обеспечивать измерения характеристик ПЭМИ в децибелах, относительно 1 мкВ, 1 мкА, 1 мкВ/м, 1 мкА/м, 1 мВт/м2.

Анализатор спектра должен быть программируемым, для дистанционного управления, т. е. должен обрабатывать команды, которые ему посылает ПЭВМ.

Должен иметь интерфейсы LAN или USB, или GPIB, или RS-232 для передачи данных с ПЭВМ на анализатор спектра и обратно.

Анализатор спектра должен иметь квазипиковый, пиковый и со среднеквадратичным отклонением детекторы.

Работать в полосе частот 9 кГц...1000 МГц.

Иметь полосы пропускания в диапазоне 1 кГц...3 МГц. Погрешность, вносимая собственными шумами, должна быть не более 1 дБ. Анализатор спектра должен обеспечивать звуковой контроль ПЭМИ, имеющих амплитудную и частотную (на частотах свыше 30 МГц) модуляцию, с помощью встроенных или подключаемых приборов или устройств.

Примерный перечень оборудования приведен в (табл. 1).

Таблица 1. Перечень оборудования для проведения оценки защищенности по каналу ПЭМИН

Наименование средств измерения	Тип	Диапазон частот
Анализатор спектра	LIGNext1 NS-30A	10 кГц -3 ГГц
Антенна магнитная рамочная активная	Н-30	10 Гц – 30 МГц
Антенна электрическая дипольная активная	Е-3000	30 МГц – 3000 МГц
Антенна электрическая дипольная активная	Е-30	10 Гц – 30 МГц
Пробник напряжения	П-400	10 Гц – 300 МГц
Осциллограф	LeCroy Wavesurfer 62Xs	0 Гц – 600 МГц
Генератор сигналов	Г4-218	200 кГц-1 ГГц

Альтернативная измерительная площадка.

Временная методика оценки защищенности ОТСС, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации (КИ), описанная в «Сборнике временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам» предполагает собой поиск и измерение опасных сигналов непосредственно на объекте информатизации.

Однако, шумовая обстановка на объекте информатизации весьма нестабильна. Помимо нестабильности она абсолютно неисследованная. Оператор при проведении измерений может столкнуться с таким явлением как «стоячая волна».

Стоячая волна (электромагнитная) – периодическое изменение амплитуды напряженности электрического и магнитного полей вдоль направления

распространения, вызванное интерференцией, падающей и отраженной волн. Например, стоячая волна возникает при отражении волны от преград и неоднородностей в результате взаимодействия (интерференции), падающей и отражённой волн.

Присутствие такой волны во время проведения измерений однозначно приведёт к ошибке.

Измерительная площадка – площадка, отвечающая требованиям, обеспечивающим правильное измерение уровней индустриальных радиопомех (ИРП), излучаемых ТС в регламентированных условиях. Видов ИП предусматриваются два – «открытая измерительная площадка» и «альтернативная измерительная площадка». Поскольку строительство и эксплуатация открытой площадки весьма дорого, сосредоточимся на более дешёвом варианте – АИП. Разница между открытой ИП и АИП заключается в том, что последняя должна размещаться не в открытом пространстве, а в некотором помещении, в здании. При том физические характеристики АИП (прежде всего «затухание» электромагнитного поля) должны оставаться в пределах установленного допуска.

Важно! Перед вводом в эксплуатацию АИП оценивается минимум искажений, вносимых в распределение электромагнитного поля ограждающими конструкциями помещения, который можно допустить. Иными словами, оператор заранее знает о наличии и характере «стоячих волн» и о характеристиках закона затухания электромагнитного поля. Это позволяет получать информацию об «опасных» информативных сигналах корректнее, чем на ОИ, на котором абсолютно не исследована шумовая обстановка.

Практическая часть.

Вопросы для самопроверки:

Назовите весь перечень оборудования для проведения оценки защищенности по ПЭМИ.

Дайте определение измерительной площадки в рамках данного задания.

Сколько существует видов измерительных площадок (ИП) и в чем их различие?

На сколько метров минимально и максимально предполагается плавное размещение антенны по высоте?

Какой должен быть коэффициент калибровки у антенн?

Практические задания:

Как по Вашему мнению вы представляете себе открытую измерительную площадку и альтернативную? Опишите их. В чем их основное различие? Ответ обоснуйте.

Представьте, что Вы начинающий сотрудник предприятия ООО «НПП «ИБЦ». Начался ваш седьмой рабочий день. Вы в обычном распорядке, получив задание, идете включать лабораторное автоматизированное рабочее место и ПАК. Неожиданным образом узнаёте, что откалиброванная антенна начала давать сбой. Вы (без особой паники) начинаете искать пути решения. По Вашему мнению, каковы основные три шага на пути решения этой проблемы? Ответ обоснуйте.

Лабораторная работа № 6.

Тема: Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам

Цель занятия: Реализация политики безопасности в КС с использованием механизмов и средств операционных систем.

Управление доступом в КС с использованием механизмов и средств сетевых операционных систем. Формирование Active Directory в ОС Windows Server 2003 (2008, 2010).

Управление инцидентами информационной безопасности в КС.

Продолжительность практического занятия-1 часа

Задание.

ЗАДАНИЕ № 1

Тема: Теоретические аспекты проведения специальных исследований (СИ) на предприятии

Цель работы.

Изучение основных принципов проведения специальных исследований на предприятии. Освоить структуру ведения общей теоретической части проведения специальных исследований.

Продолжительность занятия: полтора учебных часа.

Задания.

Изучить теоретическую часть Задания №1.

Выполнить практическую часть Задания №1:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Специальные исследования (специсследования, СИ) — комплекс действий, направленный на обнаружение потенциальных технических каналов утечки защищаемой информации с помощью специального контрольно-измерительного оборудования, в соответствии с нормативно-методическими документами ФСБ России и ФСТЭК России.

Проведение специсследований определяет возможность считывания и перехвата сигнала специальными средствами разведки в рамках определённых границ (защищённость утечек по каналам ПЭМИН — побочные электромагнитные излучения и наводки).

Введем для большей ясности определения, связанные с основой ведения специсследований на предприятии. Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается ценная информация.

Автоматизированная система (АС) – устройство или комплекс устройств, необходимых для передачи, хранения и обработки конфиденци-

альной информации, прошедшая процедуру аттестации в соответствии с законодательством РФ.

Контролируемая зона (КЗ) – пространство, в котором исключено неконтролируемое пребывание посторонних лиц или сотрудников, не имеющих прямое отношение к данному пространству. Примерами могут послужить: периметр охраняемой территории; ограждающие конструкции охраняемого здания или охраняемой территории.

Информационный сигнал – электрические сигналы, акустические, электромагнитные и т.д., по параметрам которых можно раскрыть конфиденциальную информацию, передаваемую, хранимую или обрабатываемую в основных технических средствах и системах или обсуждаемая в защищенном исполнении.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для обработки, хранения и передачи конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

Средства активной защиты информации по каналам ПЭМИН (САЗ) – технические средства формирования маскирующих электромагнитных помех в местах возможного съема защищаемой информации, прошедшие обязательную процедуру сертификации по линии ФСТЭК России.

Деятельность по технической защите конфиденциальной информации (ТЗКИ) – выполнение работ и (или) оказание услуг по ее защите:

– от несанкционированного доступа,

– от утечки по техническим каналам,

– от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Важно! Данный вид деятельности является лицензируемым. Лицензирование деятельности по ТЗКИ осуществляет ФСТЭК России.

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные поля, создаваемые в окружающем пространстве СВТ, специально для этого не предназначенными (в случае ПЭМИ) или наводки данных излучений на токоведущие конструкции, линии и подключенные к ним ТС.

Существует несколько видов проведения специсследований на определенные ТС. В данном случае это акустоэлектрическое преобразование (АЭП) и ПЭМИН. В случае АЭП исследуемое средство подвергается воздействию некоих акустических частот. Из этого обосновывается определенный вывод о возможности использования ТС на невозможности подверженности АЭП.

Как уже было указано в определениях, ПЭМИ создаются вокруг работающих технических средств, которые специально для данного излучения не создавались. То есть излучение от радиопередатчиков, мобильных телефонов – это не побочные излучения. А вот излучения при работе компьютера от монитора, принтера, накопителей информации являются побочными.

Если вспомнить физику, то вокруг проводника, по которому протекает электрический ток возникает электромагнитное поле. Если по данному проводнику передается какой-либо сигнал, то, следовательно, и электромагнитное поле тоже будет изменяться по тем же законам, что и сигнал, протекающий в линии. Таким образом, источником сигнала ПЭМИ являются все токоведущие линии в ТС, по которым в процессе работы передаются какие-либо сигналы.

Как известно электромагнитные поля могут распространяться на значительные расстояния и конструкции помещений тому не преграда. Скорость передачи данных и обработки информации в современных средствах вычислительной техники постоянно растет, а значит растут и частоты сигналов ПЭМИ. Частоты сигналов ПЭМИ могут начинаться от единиц кГц и заканчиваться единицами ГГц, а гармоники этих сигналов могут находиться еще выше по частоте.

Если вспомнить, что в проводнике, помещенном в электромагнитное поле, возникает электрический ток, то очевидно, что могут возникать наводки ПЭМИ на любые токоведущие элементы (систему отопления, короб системы вентиляции и т. д.), в том числе и любые линии и ТС, подключенные к ним, попадающие под действие данного электромагнитного поля.

Перехват этой информации можно осуществить путем анализа изменений параметров ПЭМИН с помощью специальных высокочувствительных радиоприемных устройств, оснащенных специализированными антеннами, пробниками напряжения, токосъемниками.

На (рис. 1) приведена физика утечки информации за счет ПЭМИ.

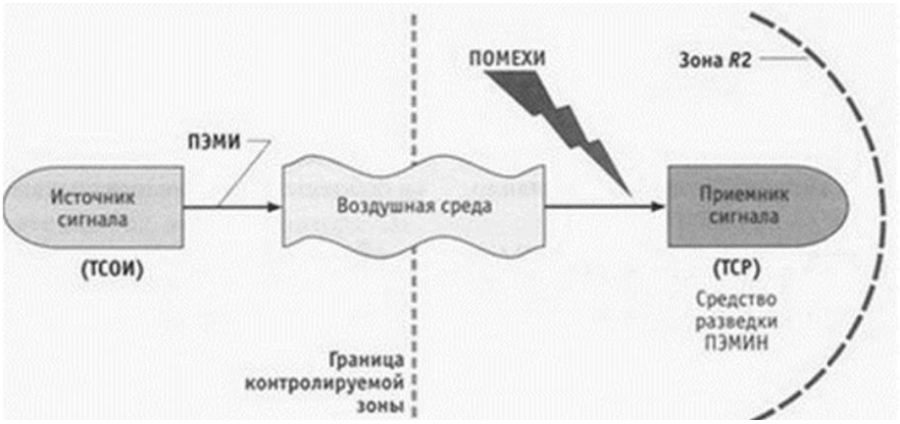


Рисунок 1. Схема ТКУИ за счет ПЭМИ

На (рис. 2) приведена физика утечки информации за счет ПЭМИН.

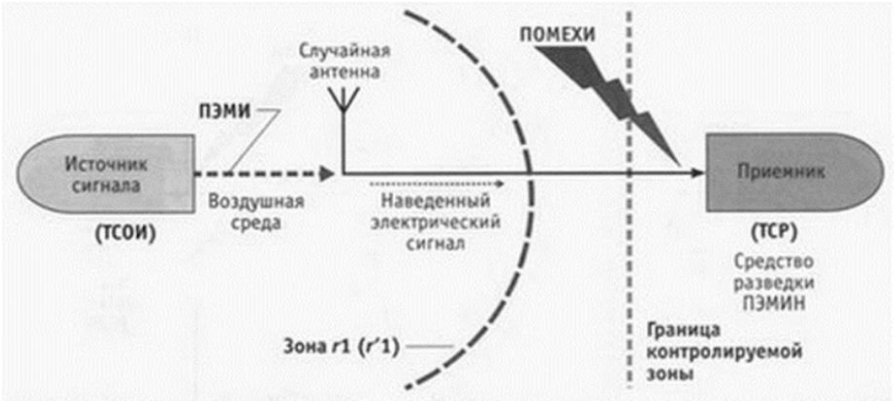


Рисунок 2. Схема ТКУИ за счет ПЭМИН

Поясним некоторые сокращения и термины на схемах:

• ТСОИ – технические средства обработки информации (все что попадает под определение ОТСС);

• ТСР–технические средства разведки;

• зона R2 – расстояние, на котором возможен перехват защищаемой информации за счет ПЭМИ;

• зона r1(r’1) – расстояние, наличие в пределах которого случайных антенн (токоведущие конструкции, линии и ТС) создает возможность утечки информации за счет наводок ПЭМИ.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенной случайной антенной может являться стационарный телефон, датчик пожарной сигнализации, громкоговоритель, подключенная к линии, выходящей за пределы КЗ.

Распределенные случайные антенным – антенны с распределенными параметрами. К ним можно отнести: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ.

Также разделяют саму информации по каналам АЭП и ПЭМИ на случай информативности. Информативные – сигналы с несущей, модулированной информативным сигналом. Примером могут послужить: сигнал от флэш-накопителя USB; VGA-интерфейс монитора; и т.д.

Неинформативные сигналы – сигналы, анализ которых не дает представления об обрабатываемой информации. Примеры: излучения от работы источников питания в узлах ТС; сигнал обработки режимов видеокартой; и т.д.

Важно! Всё приведенное выше относится к составной части по проведению работ, связанных с специальными исследованиями ОТСС и ВТСС. Однако это лишь малая часть того, что можно было бы изложить. Остальная теоретическая и прикладная часть изучается непосредственно работником предприятия в режимно секретном подразделении. Все методические материалы работ, связанных с проведением специальных исследований имеют грифы СЕКРЕТНО и СОВЕРШЕННО СЕКРЕТНО. Вышеизложенный материал является открытым и считается опорным в общих знаниях ТЗИ.

Практическая часть.

Вопросы для самопроверки:

21) Дайте определение специальным исследованиям в рамках данного учебного занятия.
22) Какие и сколько существует грифов секретности в рамках законодательства РФ?
23) Что такое зона r1(r'1) в ТЗИ?
24) Дайте определение ОТСС и ВТСС и в чем их различие?
25) На какие категории разбиваются случайные антенны в КЗ и в чем их разница? И на какие категории разбиваются информационные сигналы и в чем их разница?

Практические задания:

9) Опишите собственными словами следующие определения. ОТСС; ВТСС; ТКУИ.
10) В соответствии с (рис. 1) данного учебного задания, источником распространения сигнала ПЭМИ между техническим средством и техническим средством разведки является воздушная среда. Что будет если изменить воздушную среду на более плотную, а что, если перенести её в вакуум. Ответ обоснуйте.

Однажды, двое ученых задались очень интересной задачей, связанной с передачей информативного сигнала технического средства через канал ПЭМИ по очень интересной схеме. У них получилось и даже на современном этапе злоумышленники охотно придают значение данному средству получения заведомо важной для них информации. Двух ученых звали Маркус Кун и Росс Андерсон. При помощи сети Интернет, найдите информацию о данной процедуре получения информативного сигнала по каналу ПЭМИ и расскажите в общих чертах об этой технологии

ЗАДАНИЕ № 2

Тема: Теоретические основы средств измерения программно-аппаратных комплексов (ПАК) и альтернативной измерительной площадки (АИП)

Цель работы.

Изучение теоретической основы средств измерений сигналов. Освоить особенности поиска и идентификации сигналов при помощи альтернативной измерительной площадки.

Продолжительность занятия: полтора учебных часа.

Задания.

Изучить теоретическую часть Задания №2.

Выполнить практическую часть Задания №2:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

В связи с тем, что многие организации, занимающиеся производством и распространением программно-аппаратных комплексов, предлагают на рынке целые линейки своих продуктов, отличающихся только аппаратной частью (анализаторы спектра) и соответственно ценой на данные товары в этой линейке. На рынке представлены программ- но-аппаратные комплексы следующих производителей, распространителей: «Навигатор ПхГ» – «НЕЛК», «Сигурд Мх» – «МАСКОМ», «Легенда» – «АВМ-СИСТЕМС». Стоит отметить, что все комплексы, рассматриваемые в данной работе, имеют сертификаты ФСТЭК России и метрологический сертификат соответствия на измерительное оборудование. Пример ПАК представлен на (рис. 1).

Рисунок 1. ПАК «Сигурд М18»

Требования к антеннам.

В полосе частот от 200 Гц до 30 МГц в комплект антенн должны входить магнитная и (или) электрическая антенны.

Для измерения магнитной составляющей электромагнитного поля, антенна должна быть: электрически экранированной рамочной антенной, имеющей такие размеры, чтобы ее рамка помещалась в квадрат со стороной не более 0,6 м, или ферритовая антенна длиной не более 0,5 м.

Допускаемая погрешность измерений напряженности магнитного поля (измеритель с магнитной антенной) не должна превышать 2,5 дБ.

Конструкция антенн (антенного штатива) должна обеспечивать возможность плавного изменения высоты расположения антенны над землей от 0,8 м до 1,25 м, а также возможность поворота магнитной и электрической антенн на 360° вокруг оси.

В полосе частот от 30 до 1000 МГц в комплект антенн должны входить одна или несколько электрических антенн одного из следующих типов:

а) линейный симметричный вибратор на полосу частот от 30 до 80 МГц, размер которого равен длине полуволнового симметричного вибратора

на частоте 80 МГц, и настраиваемый полуволновой симметричный вибратор в полосе частот от 80 до 1000 МГц, имеющий КСВН не более 2,5;

б) биконическая антенна, максимальный размер которой должен быть не более 1,35 м в полосе частот от 30 до 300 МГц и с КСВН не более 3,0, и биконическая антенна, максимальный размер которой – не более 0,5 м в полосе частот от 300 до 1000 МГц с КСВН не более 2,5;

в) широкополосная антенна, главный лепесток диаграммы направленности которой должен быть таким, чтобы в направлении непосредственного излучения от источника ПЭМИН и в направлении отраженного от земли луча разность коэффициентов усиления антенны не превышала бы 1 дБ, с КСВН не более 2,5.

Конструкция антенны (антенного штатива) должна обеспечивать возможность плавного изменения высоты центра симметрии над землей от 1 до 4 м и поворота вокруг горизонтальной оси на 180°, а также фиксированную ориентацию в трех взаимно ортогональных направлениях.

Допускаемая погрешность измерений напряженности электрического поля (измеритель с биконической, электрической антенной) не должна превышать 2,5 дБ на частотах до 1000 МГц.

Антенны должны иметь коэффициент калибровки, позволяющий измерять уровни полей. Рекомендуемый коэффициент калибровки антенн – не более 40 дБ. Погрешность коэффициента калибровки антенн должна быть не более 2 дБ.

Требования к анализатору.

Должен иметь несимметричный вход с номинальным значением сопротивления 50 Ом с коэффициентом стоячей волны по напряжению (КСВН) не более 2 при ослаблении входного аттенюатора 0 дБ и не более 1,2 при ослаблении входного аттенюатора 10 дБ и более.

Измерители совместно с первичными преобразователями должны обеспечивать измерения характеристик ПЭМИ в децибелах, относительно 1 мкВ, 1 мкА, 1 мкВ/м, 1 мкА/м, 1 мВт/м2.

Анализатор спектра должен быть программируемым, для дистанционного управления, т. е. должен обрабатывать команды, которые ему посылает ПЭВМ.

Должен иметь интерфейсы LAN или USB, или GPIB, или RS-232 для передачи данных с ПЭВМ на анализатор спектра и обратно.

Анализатор спектра должен иметь квазипиковый, пиковый и со среднеквадратичным отклонением детекторы.

Работать в полосе частот 9 кГц...1000 МГц.

Иметь полосы пропускания в диапазоне 1 кГц...3 МГц. Погрешность, вносимая собственными шумами, должна быть не более 1 дБ. Анализатор спектра должен обеспечивать звуковой контроль ПЭМИ, имеющих амплитудную и частотную (на частотах свыше 30 МГц) модуляцию, с помощью встроенных или подключаемых приборов или устройств.

Примерный перечень оборудования приведен в (табл. 1).

Таблица 1. Перечень оборудования для проведения оценки защищенности по каналу ПЭМИН

Наименование средств измерения	Тип	Диапазон частот
Анализатор спектра	LIGNext1 NS-30A	10 кГц -3 ГГц
Антенна магнитная рамочная активная	Н-30	10 Гц – 30 МГц
Антенна электрическая дипольная активная	Е-3000	30 МГц – 3000 МГц
Антенна электрическая дипольная активная	Е-30	10 Гц – 30 МГц
Пробник напряжения	П-400	10 Гц – 300 МГц
Осциллограф	LeCroy Wavesurfer 62Xs	0 Гц – 600 МГц
Генератор сигналов	Г4-218	200 кГц-1 ГГц

Альтернативная измерительная площадка.

Временная методика оценки защищенности ОТСС, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации (КИ), описанная в «Сборнике временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам» предполагает собой поиск и измерение опасных сигналов непосредственно на объекте информатизации.

Однако, шумовая обстановка на объекте информатизации весьма нестабильна. Помимо нестабильности она абсолютно неисследованная. Оператор при проведении измерений может столкнуться с таким явлением как «стоячая волна».

Стоячая волна (электромагнитная) – периодическое изменение амплитуды напряженности электрического и магнитного полей вдоль направления распространения, вызванное интерференцией, падающей и отраженной волн. Например, стоячая волна возникает при отражении волны от преград и неоднородностей в результате взаимодействия (интерференции), падающей и отражённой волн.

Присутствие такой волны во время проведения измерений однозначно приведёт к ошибке.

Измерительная площадка – площадка, отвечающая требованиям, обеспечивающим правильное измерение уровней индустриальных радиопомех (ИРП), излучаемых ТС в регламентированных условиях. Видов ИП предусматриваются два – «открытая измерительная площадка» и «альтернативная измерительная площадка». Поскольку строительство и эксплуатация открытой площадки весьма дорого, сосредоточимся на более дешёвом варианте – АИП. Разница между открытой ИП и АИП заключается в том, что последняя должна размещаться не в открытом пространстве, а в некотором помещении, в здании. При том физические характеристики АИП (прежде всего «затухание» электромагнитного поля) должны оставаться в пределах установленного допуска.

Важно! Перед вводом в эксплуатацию АИП оценивается минимум искажений, вносимых в распределение электромагнитного поля ограждающими конструкциями помещения, который можно допустить. Иными словами, оператор заранее знает о наличии и характере «стоячих волн» и о характеристиках закона затухания электромагнитного поля. Это позволяет получать информацию об «опасных» информативных сигналах корректнее, чем на ОИ, на котором абсолютно не исследована шумовая обстановка.

Практическая часть.

Вопросы для самопроверки:

Назовите весь перечень оборудования для проведения оценки защищенности по ПЭМИ.

Дайте определение измерительной площадки в рамках данного задания.

Сколько существует видов измерительных площадок (ИП) и в чем их различие?

На сколько метров минимально и максимально предполагается плавное размещение антенны по высоте?

Какой должен быть коэффициент калибровки у антенн?

Практические задания:

Как по Вашему мнению вы представляете себе открытую измерительную площадку и альтернативную? Опишите их. В чем их основное различие? Ответ обоснуйте.

Представьте, что Вы начинающий сотрудник предприятия ООО «НПП «ИБЦ». Начался ваш седьмой рабочий день. Вы в обычном распорядке, получив задание, идете включать лабораторное автоматизированное рабочее место и ПАК. Неожиданным образом узнаёте, что откалиброванная антенна начала давать сбой. Вы (без особой паники)

начинаете искать пути решения. По Вашему мнению, каковы основные три шага на пути решения этой проблемы? Ответ обоснуйте.

Лабораторная работа № 7.
Тема: Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации

Цель занятия: Построение систем защиты от угрозы нарушения конфиденциальности Реализация идентификации и аутентификации в ОС. Стойкость системы идентификации и аутентификации. Блок-схема идентификации и аутентификации. Многофакторная аутентификация.

Особенности построения парольных систем аутентификации. Парольная защита. Понятия идентификатора и пароля пользователя. Учетная запись пользователя как совокупность его идентификатора и его пароля. Парольная система и состав её элементов. Основные угрозы безопасности парольных систем. Способы получения пароля злоумышленником. Рекомендации по практической реализации парольных систем. Оценка стойкости парольных систем. Методы хранения и передачи паролей. Механизмы хранения паролей в КС.

Проблема организации совместного доступа различных приложений к некоторым областям памяти. Основные способы защиты памяти. Барьерные адреса. Механизм функционирования барьерного способа защиты памяти. Способы задания барьерного адреса. Динамические области памяти. Защита данных приложений.

Адресные регистры. Особенности способов защиты памяти. Ключ доступа. Организация совместного использования областей памяти. Механизм страничной организации памяти и сегментации. Цифровая подпись. Проблема аутентификации данных или цифровой подписи. Модель аутентификации сообщений. Сравнительный анализ обычной и цифровой подписи.

Защита от угрозы целостности на уровне содержания информации как защита от дезинформации. Наиболее распространенные приёмы использования дезинформации. Условия успешной борьбы с вероятной дезинформацией. Различие фактов и мнений. Применение дублирующих каналов. Причины актуальности проблема защиты информации в АС от угрозы нарушения целостности на уровне содержания информации. Примеры простейшей смысловой проверки.

Продолжительность практического занятия-1 часа

Задание.

ЗАДАНИЕ № 3

Тема: Определение ПЭМИ на примере информативного сигнала видеотракта

Цель работы.

Изучение теоретической основы измерений ПЭМИ на примере показателей информативного сигнала видеотракта. Изучение основных аспектов проведения специальных исследований.

Продолжительность занятия: полтора учебных часа.

Задания.

Изучить теоретическую часть Задания №3.

Выполнить практическую часть Задания №3:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Одним из основных и, зачастую, самых мощных источников сигналов ПЭМИ является видеотракт. Конечно сигнал, который нас интересует, это сигнал интерфейса передачи видеосигнала, но все устройства видеотракта, включающие видеоконтроллер, соединительные кабели, KVM коммутаторы (для систем с несколькими устройствами отображения информации) и конечные устройства отображения (мониторы, прокторы, телевизоры) существенно влияют на уровень сигнала и направление его излучения, потому как выступают в качестве антенн.

Приведем список наиболее популярных видео-интерфейсов: аналоговый:

- VGA (несмотря на широкое развитие современных цифровых

интерфейсов имеет широкое распространение и еще долгое время будет эксплуатироваться на большинстве АС);

цифровые:

• DVI (бывает совмещен с VGA и применяются переходники VGADVI, в таком случае рассматривается как VGA);

• HDMI;

• DisplayPort.

Немного забегая вперед, для анализа интерфейса рассмотрим один из способов определения частот сигналов ПЭМИ – непосредственное подключение к линии передачи сигнала, путем использования специального кабеля с выводами для подключения. Рассмотрение будем вести на примере VGA интерфейса в силу простоты сигнала, схожего с телевизионным, а также стабильности и понятности задания тестового режима. Не имеет значения к какому из проводов, передающих цвет (R, G или B) подключаться, так как при формировании тестового режима, обеспечивающего максимальную частоту следования импульсов, на экран монитора выводится статическая засветка пиксель белый, пиксель черный, пиксель белый и т. д. При формировании белой точки сигнал присутствует в проводе каждого из цветов (рис. 1).

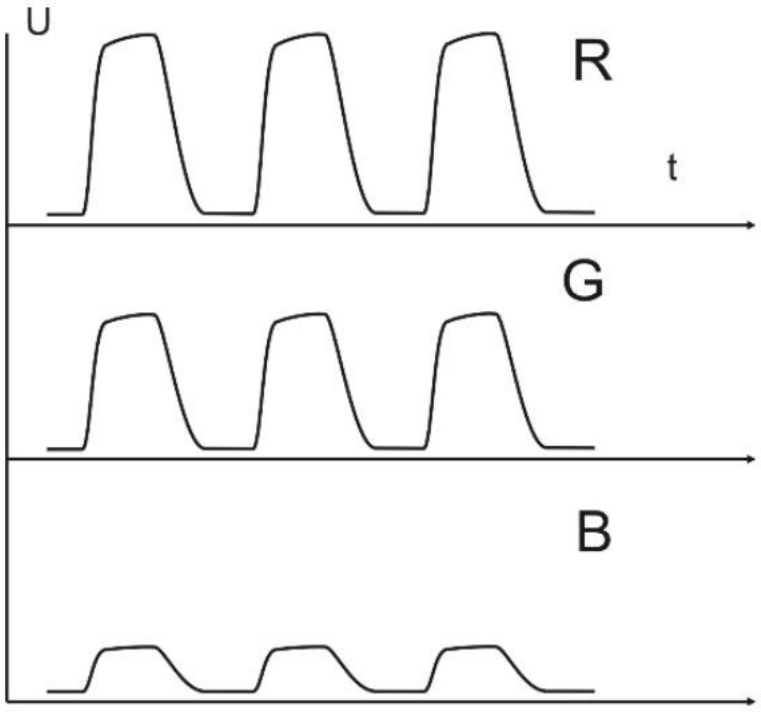
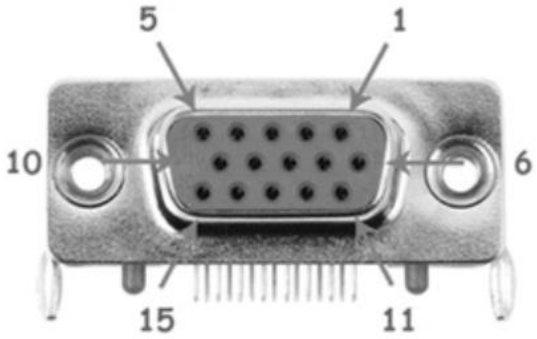


Рисунок 1. Осциллограммы сигналов в RGB интерфейсе

Распиновка разъема VGA информационного кабеля приведена на (рис. 2)



№	Наименование	Описание
1	RED	Красный сигнал
2	GREEN	Зеленый сигнал
3	BLUE	Синий сигнал
4	n/c	Не используется
5	GND	Земля
6	RED_RTN	Красный земля
7	GREEN_RTN	Зеленый земля
8	BLUE_RTN	Синий земля
9	VDC	+5В
10	GND	Земля
11	ID0	Идентификатор монитора
12	SDA	DDC / I2C data
13	HSYNC	Горизонтальная синхронизация
14	VSYNC	Вертикальная синхронизация
15	SCL	DDC / I2C clock

Рисунок 2. Распиновка разъема информационного кабеля VGA интерфейса

Кабель для данного вида исследований изготавливается специально и используется исключительно для определения частот сигналов ПЭМИ VGA интерфейса, измерения необходимо строго производить именно с тем кабелем, с которым будет эксплуатироваться АС. Структура сигнала представляется следующим образом.

С кадровой частотой (например, 60 Гц) следуют «пачки» импульсов, формирующих каждый кадр на экране монитора (рис. 3).

Кадровые «пачки» импульсов состоят в свою очередь из строчных последовательностей импульсов, каждая из которых задает сигнал для форми-

рования строки на экране монитора (частота следования при разрешении 1024 × 768 в 768 чаще, чем кадровая, то есть около 46 кГц, рис. 4).

Строчные «пачки» импульсов состоят уже непосредственно из импульсов с переходами из 0 в 1, соответствующим тестовому режиму (пиксель белый, пиксель черный и т. д.).

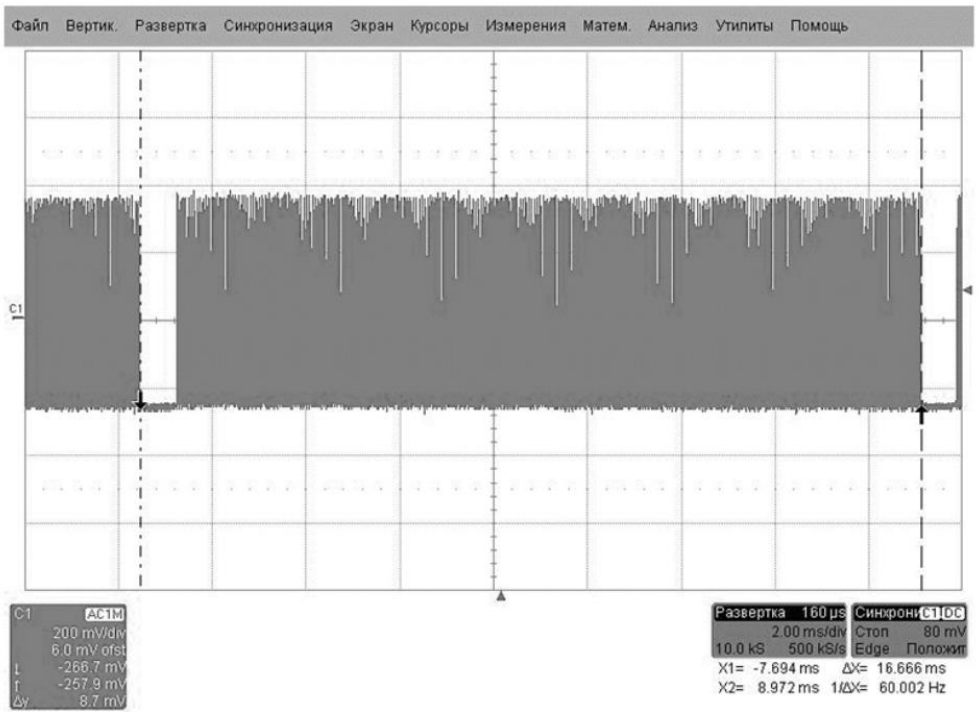


Рисунок 3. Кадровые видеоимпульсы

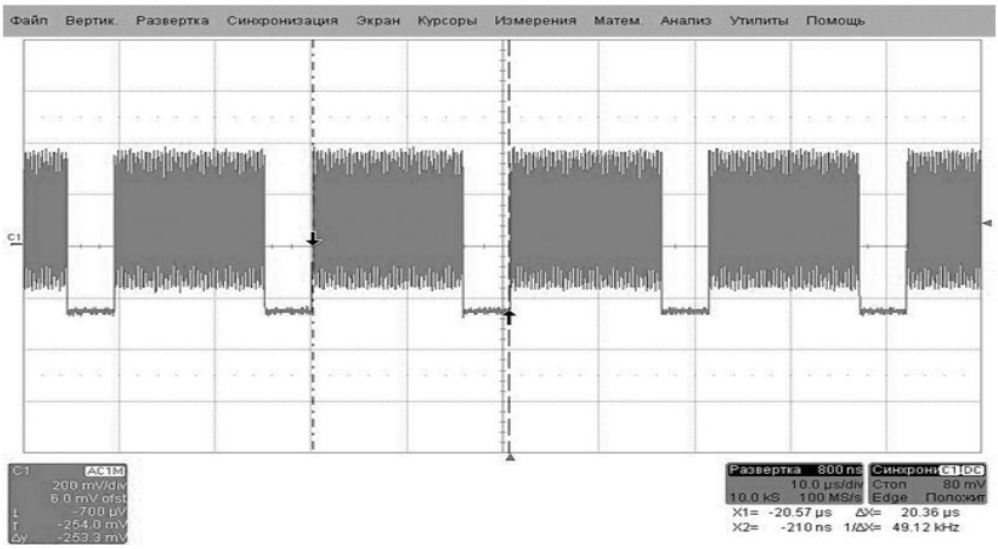


Рисунок 4. «Пачки» строчных видеоимпульсов

В результате, частота следования импульсов, задающих черные и белые пиксели и будет тактовой частотой (частотой первой гармоники) нашего сигнала ПЭМИ от видеотракта (в данном случае 32,5 МГц, можно также для уточнения применять режим БПФ). Следует отметить, что подобные кабели (с отводами для подключения осциллографа) используются только на этапе анализа сигналов, при измерениях необходимо в обязательном порядке применять кабели, с которыми в дальнейшем будет эксплуатироваться данная АС.

Сложнее дело обстоит с цифровыми видео интерфейсами, например, DVI, в основе которого лежит технология TMDS. Суть данной технологии заключается в том, что на каждый цвет приходится по две пары. Воздействие возможных помех будет производиться одинаково на оба провода, а, следовательно, их можно будет легко отфильтровать. Также в интерфейсе применяется технология минимизации количества переходов из «0» в «1» (и наоборот), что также сказывается на помехозащищенности интерфейса.

К сожалению, все это усложняет задачу для формирования тестового сигнала, который, наоборот, должен обеспечивать максимальную частоту следования импульсов в канале. У протокола TMDS есть одна особенность. Если длительное время передается сплошной поток «1», то в силу того, что кабель обладает определенной емкостью, спад уровня с «1» до «0» может произойти с задержкой, следовательно, произойдет потеря пакетов. Для того чтобы этого избежать, в таких ситуациях, протокол TMDS в конце каждых 8 битов добавляет бит DC-Balancing, который указывает на что, что следующие 8 битов будут инвертированы. В результате получаем последовательность импульсов с постоянными и стабильными переходами. Тактовая частота первой гармоники DVI интерфейса при данном тестовом режиме и стандартных разрешениях не выше 1600 × 1280 × 60 Гц лежит в пределах 130...170 МГц.

Интерфейсы HDMI и DisplayPort строятся также с применением технологии TMDS, но с увеличением скорости передачи данных, способ задания

тестового режима остается такой же, только тактовые частоты будут гораздо выше, возможно даже за пределами исследуемого нами диапазона частот.

Практическая часть.

Вопросы для самопроверки:

Что такое видеоинтерфейс?

Какие интерфейсы есть у информационного кабеля для видео? Перечислите.

Чем отличаются кадровые «пачки» импульсов от строчных?

Какая частота приемлема для видео с интерфейсом VGA?

С каким видеоинтерфейсом больше всего возникает проблем при измерении?

Практические задания:

На Ваш взгляд, что нужно сделать при проведении измерений видеосигнала? Опишите начало измерений от получения технического средства для проведения исследований до передачи его обратно в комплект поставки. Для данного задания можете попросить помощи у Вашего преподавателя.

Как Вы считаете, что такое меандр информативного сигнала? Опишите это явление на примере информативного сигнала монитора с интерфейсом VGA.

Лабораторная работа № 8.
Тема: Методология обследования и проектирования защищенных информационных (автоматизированных) систем

Цель занятия: Обследование информационных (автоматизированных) систем на соответствие требованиям ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения.

Проектирование защищенных информационных (автоматизированных) систем в соответствии с ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования.

Методы защиты информационных параметров. Модификация как метод защиты исполняемого кода программы. Способы модификации кода.
Программы-упаковщики. Использование нестандартных упаковщиков. Шифрование тела программы и данных. Выбор ключа к шифру.
Нерегламентированная передача управления. Использование нестандартных точек и способов входа в обработчики прерываний. Методы противодействия отладчикам. Различные способы модификации кода при работе программы.
Особенности реализации системы защиты КС от угрозы раскрытия параметров системы. Условия обеспечения доступа к содержанию информации злоумышленником. Необходимое условие для считывания информации с магнитного носителя информации (МНИ). Меры защиты, направленные на противодействие злоумышленнику.
Процедура определения формата носителя на логическом уровне. Способы идентификации злоумышленником МНИ. Основной критерий осуществления злоумышленником логического доступа к информации. Стандарты оформления (форматы) файлов. Задача выявления смысла содержимого файла.
Продолжительность практического занятия-1 часа
Задание.

ЗАДАНИЕ № 3

Тема: Определение ПЭМИ на примере информативного сигнала видеотракта

Цель работы.

Изучение теоретической основы измерений ПЭМИ на примере показателей информативного сигнала видеотракта. Изучение основных аспектов проведения специальных исследований.

Продолжительность занятия: полтора учебных часа.

Задания.

Изучить теоретическую часть Задания №3.

Выполнить практическую часть Задания №3:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Одним из основных и, зачастую, самых мощных источников сигналов ПЭМИ является видеотракт. Конечно сигнал, который нас интересует, это сигнал интерфейса передачи видеосигнала, но все устройства видеотракта, включающие видеоконтроллер, соединительные кабели, KVM коммутаторы (для систем с несколькими устройствами отображения информации) и конечные устройства отображения (мониторы, прокторы, телевизоры) существенно влияют на уровень сигнала и направление его излучения, потому как выступают в качестве антенн.

Приведем список наиболее популярных видео-интерфейсов: аналоговый:

- VGA (несмотря на широкое развитие современных цифровых

интерфейсов имеет широкое распространение и еще долгое время будет эксплуатироваться на большинстве АС);

цифровые:

- DVI (бывает совмещен с VGA и применяются переходники VGADVI, в таком случае рассматривается как VGA);
- HDMI;
- DisplayPort.

Немного забегая вперед, для анализа интерфейса рассмотрим один из способов определения частот сигналов ПЭМИ – непосредственное подключение к линии передачи сигнала, путем использования специального кабеля с выводами для подключения. Рассмотрение будем вести на примере VGA интерфейса в силу простоты сигнала, схожего с телевизионным, а также стабильности и понятности задания тестового режима. Не имеет значения к какому из проводов, передающих цвет (R, G или B) подключаться, так как при формировании тестового режима, обеспечивающего максимальную частоту следования импульсов, на экран монитора выводится статическая засветка пиксель белый, пиксель черный, пиксель белый и т. д. При формировании белой точки сигнал присутствует в проводе каждого из цветов (рис. 1).

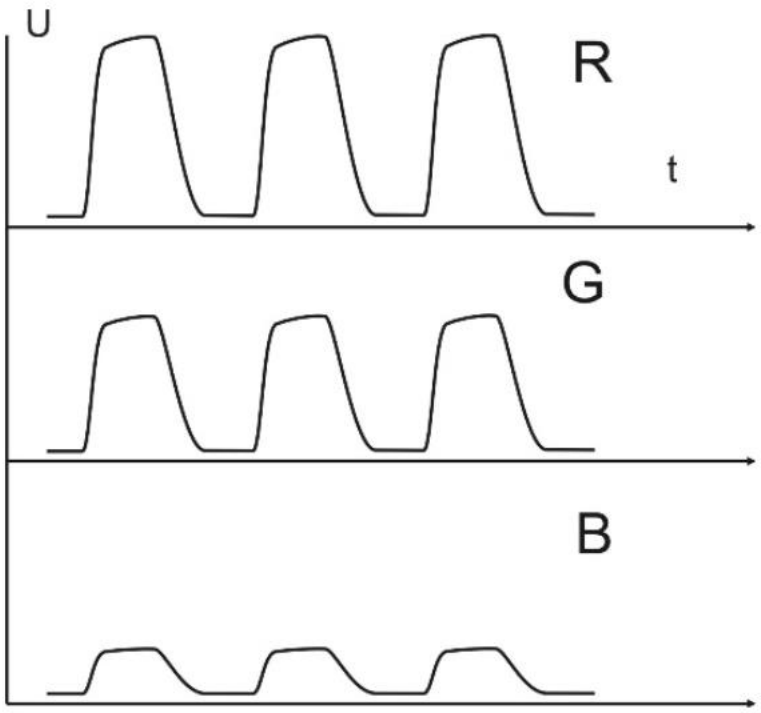
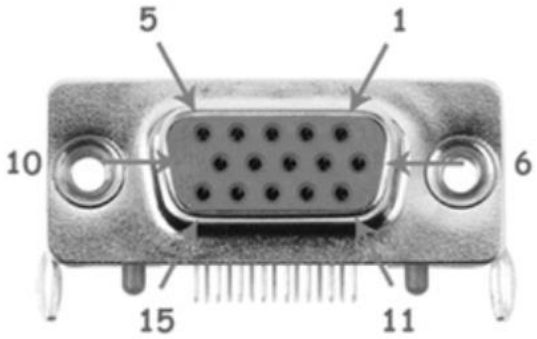


Рисунок 1. Осциллограммы сигналов в RGB интерфейсе

Распиновка разъема VGA информационного кабеля приведена на (рис. 2)



№	Наименование	Описание
1	RED	Красный сигнал
2	GREEN	Зеленый сигнал
3	BLUE	Синий сигнал
4	n/c	Не используется
5	GND	Земля
6	RED_RTN	Красный земля
7	GREEN_RTN	Зеленый земля
8	BLUE_RTN	Синий земля
9	VDC	+5В
10	GND	Земля
11	ID0	Идентификатор монитора
12	SDA	DDC / I2C data
13	HSYNC	Горизонтальная синхронизация
14	VSYNC	Вертикальная синхронизация
15	SCL	DDC / I2C clock

Рисунок 2. Распиновка разъема информационного кабеля VGA интерфейса

Кабель для данного вида исследований изготавливается специально и используется исключительно для определения частот сигналов ПЭМИ VGA интерфейса, измерения необходимо строго производить именно с тем кабелем, с которым будет эксплуатироваться АС. Структура сигнала представляется следующим образом.

С кадровой частотой (например, 60 Гц) следуют «пачки» импульсов, формирующих каждый кадр на экране монитора (рис. 3).

Кадровые «пачки» импульсов состоят в свою очередь из строчных последовательностей импульсов, каждая из которых задает сигнал для формирования строки на экране монитора (частота следования при разрешении 1024 × 768 в 768 чаще, чем кадровая, то есть около 46 кГц, рис. 4).

Строчные «пачки» импульсов состоят уже непосредственно из импульсов с переходами из 0 в 1, соответствующим тестовому режиму (пиксель белый, пиксель черный и т. д.).

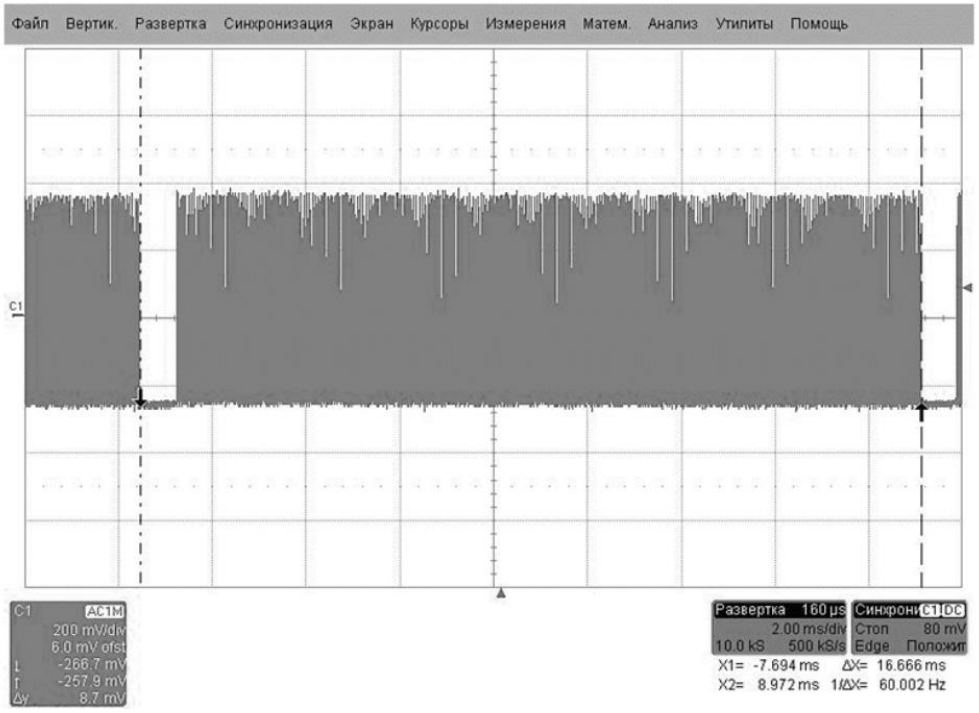


Рисунок 3. Кадровые видеоимпульсы

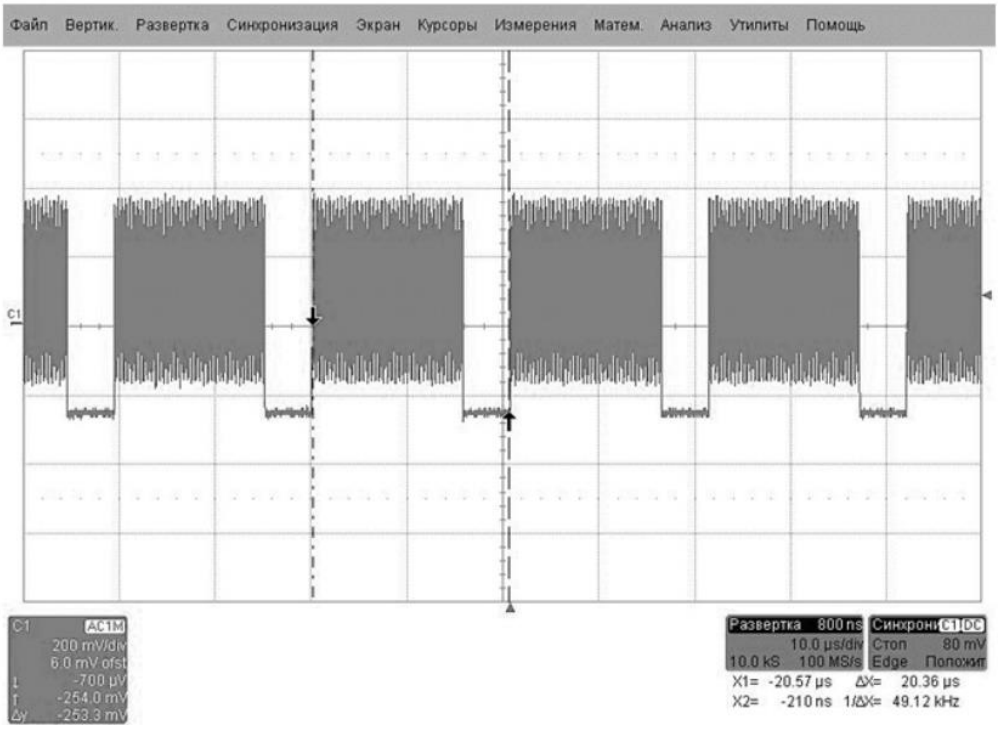


Рисунок 4. «Пачки» строчных видеоимпульсов

В результате, частота следования импульсов, задающих черные и белые пиксели и будет тактовой частотой (частотой первой гармоники) нашего сигнала ПЭМИ от видеотракта (в данном случае 32,5 МГц, можно также для уточнения применять режим БПФ). Следует отметить, что подобные кабели (с отводами для подключения осциллографа) используются только на этапе анализа сигналов, при измерениях необходимо в обязательном порядке применять кабели, с которыми в дальнейшем будет эксплуатироваться данная АС.

Сложнее дело обстоит с цифровыми видео интерфейсами, например, DVI, в основе которого лежит технология TMDS. Суть данной технологии заключается в том, что на каждый цвет приходится по две пары. Воздействие возможных помех будет производиться одинаково на оба провода, а, следовательно, их можно будет легко отфильтровать. Также в интерфейсе применяется технология минимизации количества переходов из «0» в «1» (и наоборот), что также сказывается на помехозащищенности интерфейса.

К сожалению, все это усложняет задачу для формирования тестового сигнала, который, наоборот, должен обеспечивать максимальную частоту следования импульсов в канале. У протокола TMDS есть одна особенность. Если длительное время передается сплошной поток «1», то в силу того, что кабель обладает определенной емкостью, спад уровня с «1» до «0» может произойти с задержкой, следовательно, произойдет потеря пакетов. Для того чтобы этого избежать, в таких ситуациях, протокол TMDS в конце каждых 8 битов добавляет бит DC-Balancing, который указывает на что, что следующие 8 битов будут инвертированы. В результате получаем последовательность импульсов с постоянными и стабильными переходами. Тактовая частота первой гармоники DVI интерфейса при данном тестовом режиме и стандартных разрешениях не выше 1600 × 1280 × 60 Гц лежит в пределах 130...170 МГц.

Интерфейсы HDMI и DisplayPort строятся также с применением технологии TMDS, но с увеличением скорости передачи данных, способ задания

тестового режима остается такой же, только тактовые частоты будут гораздо выше, возможно даже за пределами исследуемого нами диапазона частот.

Практическая часть.

Вопросы для самопроверки:

1) Что такое видеоинтерфейс?
2) Какие интерфейсы есть у информационного кабеля для видео? Перечислите.
3) Чем отличаются кадровые «пачки» импульсов от строчных?
4) Какая частота приемлема для видео с интерфейсом VGA?
5) С каким видеоинтерфейсом больше всего возникает проблем при измерении?

Практические задания:

1) На Ваш взгляд, что нужно сделать при проведении измерений видеосигнала? Опишите начало измерений от получения технического средства для проведения исследований до передачи его обратно в комплект поставки. Для данного задания можете попросить помощи у Вашего преподавателя.
2) Как Вы считаете, что такое меандр информативного сигнала? Опишите это явление на примере информативного сигнала монитора с интерфейсом VGA.

Лабораторная работа № 9.
Тема: Общие сведения о стандартах в области информационной безопасности

Цель занятия: Классификация стандартов в области ИБ. Оценочные стандарты в области ИБ. Назначение оценочных стандартов в области ИБ. Состав оценочных стандартов.

Критерии безопасности компьютерных систем. Уровни безопасности. Спецификации. Назначение и состав спецификаций.

Основные направления реализации и использования средств и методов защиты в КС. Практические вопросы управления информационной безопасностью

организаций. Процедура сертификации продуктов и систем, применяемых в КС.
Основные механизмы обеспечения совместимости продуктов и систем. Стандартизация набора требований безопасности. Условия для оценки эффективности средств компьютерной безопасности.
Продолжительность практического занятия-1 часа
Задание.

ЗАДАНИЕ № 4

Тема: Средства защиты информации

Цель работы.

Изучение теоретической основы активных средств защиты. Изучение основных аспектов настройки и эксплуатации средств защиты.

Продолжительность занятия: полтора учебных часа.

Задания.

Изучить теоретическую часть Задания №4.

Выполнить практическую часть Задания №4:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Целью защиты информации от утечки по ТКУИ является уменьшение отношения «сигнал/шум». Уменьшение может осуществляться с помощью применения пассивных и/или активных методов и средств защиты.

Активный метод заключается в перекрытии полезного сигнала более мощным шумом. Данный метод защиты осуществляется аппаратное, через специальные устройства так называемые «Генератор шума». Генераторы шумов специально создают мощные электромагнитные излучения, которые не имеют информативной ценности и затрудняют или делают совсем невозможным анализ полезного сигнала относительно окружающего шума. Надо

заметить, что генераторы шумов от побочных электромагнитных излучений имеют свои недостатки, такие как:

- довольно мощные источники излучения не являются полезным для здоровья;
- наличие маскирующего сигнала говорит о наличие конфиденциальной информации;
- нельзя гарантировать абсолютную защищенность информации.

Пассивный метод заключается в уменьшении мощности самого излучаемого сигнала. Осуществление подобного метода заключается в изоляции излучающих проводников, устройств, а также периметра помещения специальными материалами поглощающими ЭМП, в отношении проводных линий – установка фильтров.

Активные методы основаны на увеличении уровня шума путем применения генераторов пространственного зашумления. Данные устройства, как правило, формируют широкополосную помеху во всем диапазоне частот. Регулировка в большинстве моделей осуществляется только по общему уровню сигнала, за редким исключением присутствует возможность корректировки частотной характеристики на низких, средних и высоких частотах.

С точки зрения заключения договора на аттестацию ОИ применение САЗ самый удобный и простой вариант, а иногда и единственный (если организация арендует 1-2 помещения и расстояние до границы КЗ 1 м).

Наиболее популярные модели САЗ по каналу ПЭМИН приведены. приведен скан сертификата ФСТЭК России на САЗ «Соната-Р3.1».

Рисунок 1. Средство активной защиты от утечек за счет ПЭМИН «Соната-Р3.1»

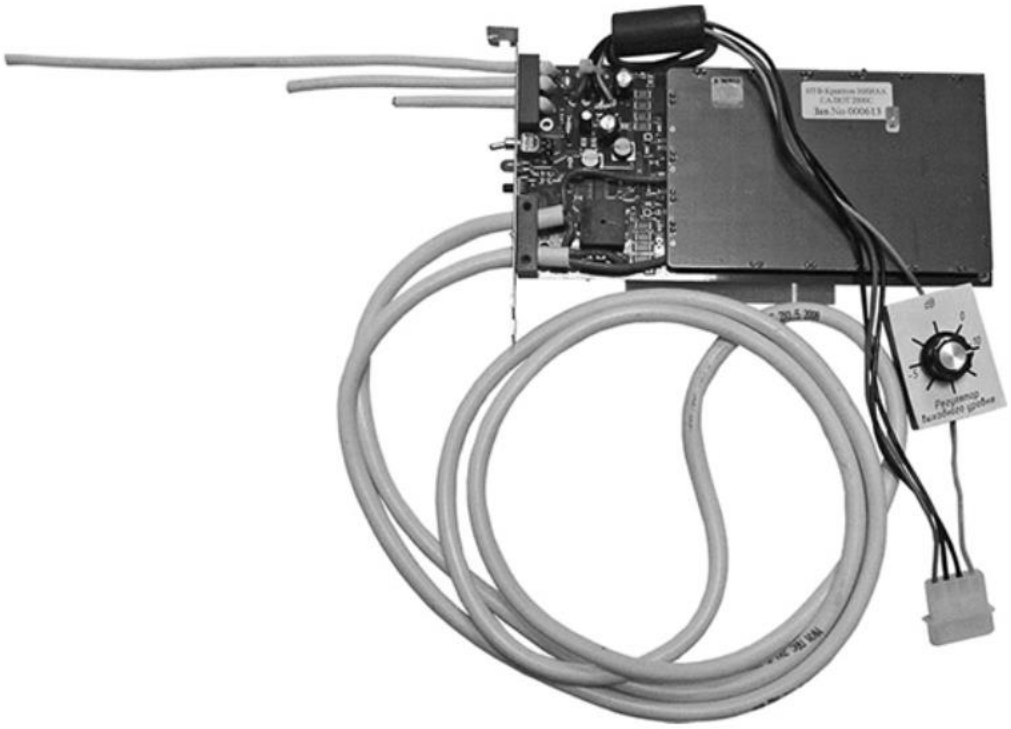
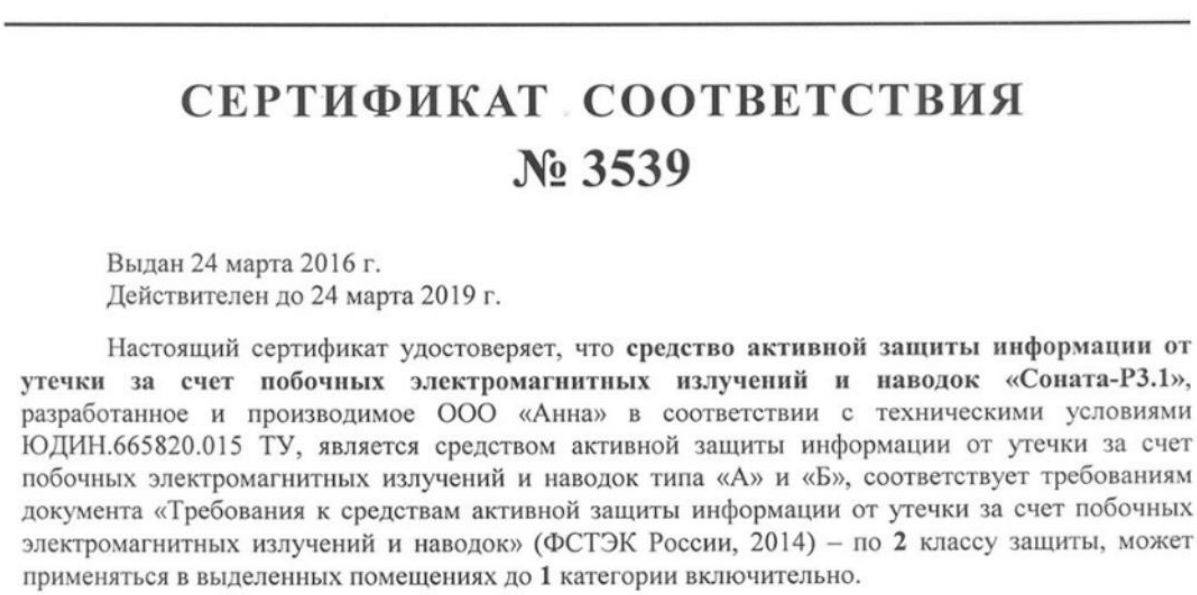


Рисунок 2. Средство активной защиты информации от утечек за счет ПЭМИН «Салют 2000С»



СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3539

Выдан 24 марта 2016 г.
Действителен до 24 марта 2019 г.

Настоящий сертификат удостоверяет, что **средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «Соната-Р3.1»**, разработанное и производимое ООО «Анна» в соответствии с техническими условиями ЮДИН.665820.015 ТУ, является средством активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок типа «А» и «Б», соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) – по **2** классу защиты, может применяться в выделенных помещениях до **1** категории включительно.

Рисунок 3. Сертификат соответствия ФСТЭК России на СЗИ «Соната-Р3.1»

Исходя из графика спектров помех можно сделать вывод, что во всем диапазоне частот помехи не обладают равномерным спектром. Вследствие чего, при проведении измерений, сигналы ПЭМИ могут оказаться на частотах, соответствующих «провалам» в спектре помехи, что поставит под вопрос защищенность объекта. Проблема в том, что с точки зрения требований по сертификации САЗ по каналу ПЭМИН, оценивается только спектральная плотность мощности, причем в достаточно широкой полосе, а то, как ведет себя спектр помехи в данной полосе это уже будет видно на практике (для примера приведем характеристики САЗ «Соната-Р2», табл. 2–4).

Таблица 2

Спектральная плотность напряженности электрической составляющей ЭМП «Соната-Р2», не менее

Диапазон частот, МГц	Вертикальная поляризация, дБ		Горизонтальная поляризация, дБ	
	Без дополнительной антенны	С дополнительной антенной	Без дополнительной антенны	С дополнительной антенной
от 0,01 до 0,15	50	80	50	80
от 0,15 до 1	45	70	40	70
от 1 до 5	45	60	40	55
от 5 до 30	45	60	40	50
от 30 до 100	40	50	40	50
от 100 до 1000	30	30	30	30
от 1000 до 2000	30	30	30	30

Таблица 3

Спектральная плотность напряженности магнитной составляющей ЭМП «Соната-Р2», не менее

Диапазон частот, МГц	Без дополнительной антенны, дБ	С дополнительной антенной, дБ
от 0,01 до 0,15	30	30
от 0,15 до 4	35	35
от 4 до 10	40	40
от 10 до 30	30	35

Таблица 4

Спектральная плотность напряжения помех в линиях электропитания и заземления «Соната-Р2», не менее

Диапазон частот, МГц	Без дополнительной антенны, дБ	С дополнительной антенной, дБ
от 0,01 до 0,04	25	25
от 0,04 до 10	35	35
от 10 до 100	35	45
от 100 до 600	25	25
от 600 до 1000	15	15

Пассивные методы защиты информации от утечки по каналам ПЭМИН возможно реализовать следующими путями:

- уменьшение уровня информативного сигнала за счет экранирования помещения (что практически невозможно, гарантию может дать только специализированная экран камера, которая применяется для лабораторных исследований источников радиосигналов).
- если в процессе анализа выявлено, что ТКУИ возникает только за счет наводок на линии электропитания, то возможно применение сетевых подавляющих фильтров (рисунок 3).

Рисунок 3. Фильтр сетевой помехоподавляющий ЛФС-10-1Ф

Фильтр сетевой помехоподавляющий ЛФС-10-1Ф предназначен для защиты информации, обрабатываемой техническими средствами и системами и содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа от утечки по каналам побочных электромагнитных наводок на линии электропитания напряжением 220 В с частотой 50 Гц

«ЛФС-10-1Ф» соответствует: типу – пассивные средства защиты информации от утечки за счет побочных электромагнитных наводок на линии электропитания.

«ЛФС-10-1Ф» соответствует документу «Требования к пассивным средствам защиты информации от побочных электромагнитных наводок на линии электропитания» (ФСТЭК России, 2015), – по 1 классу защиты.

Отметим, что на практике чаще всего в случае невыполнения норм защищенности применяются средства активной защиты – генераторы электромагнитного шума, которые также создают наведенную помеху на линии и токоведущие коммуникации.

Практическая часть.

Вопросы для самопроверки:

6) Опишите самый простой и удобный способ на аттестацию ОИ при применении САЗ.
7) По какому классу защиты соответствует ЛФС-10-1Ф?
8) Что такое активная защита САЗ?
9) Что такое пассивная защита САЗ?
10) Какими методами по защите информации от утечек ПЭМИН возможно реализовать пассивные меры защиты?

Практические задания:

3) По вашему мнению, является ли допустимым использование одновременно и пассивных и активных мер защиты? Если возможно, в подробности расскажите почему?

Лабораторная работа № 10. Концепция защиты СВТ и АС от НСД в соответствии с руководящими документами Гостехкомиссии и нормативно-методическими документами ФСТЭК России

Цель занятия: Классификация межсетевых экранов (МЭ) по уровню защищённости от НСД к информации. Классы и показатели защищённости МЭ.
Программное обеспечение (ПО) средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Понятие недекларированных возможностей.
Программные закладки как возможные реализации недекларированных возможностей. Уровни контроля. Основные категории проверок. Статический и динамический анализ.
Продолжительность практического занятия-1 часа
Задание.

ЗАДАНИЕ № 4

по дисциплине

Тема: Средства защиты информации

Цель работы.

Изучение теоретической основы активных средств защиты. Изучение основных аспектов настройки и эксплуатации средств защиты.

Продолжительность занятия: полтора учебных часа.

Задания.

Изучить теоретическую часть Задания №4.

Выполнить практическую часть Задания №4:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Целью защиты информации от утечки по ТКУИ является уменьшение отношения «сигнал/шум». Уменьшение может осуществляться с помощью применения пассивных и/или активных методов и средств защиты.

Активный метод заключается в перекрытии полезного сигнала более мощным шумом. Данный метод защиты осуществляется аппаратное, через специальные устройства так называемые «Генератор шума». Генераторы шумов специально создают мощные электромагнитные излучения, которые не имеют информативной ценности и затрудняют или делают совсем невозможным анализ полезного сигнала относительно окружающего шума. Надо заметить, что генераторы шумов от побочных электромагнитных излучений имеют свои недостатки, такие как:

- довольно мощные источники излучения не являются полезным для здоровья;

• наличие маскирующего сигнала говорит о наличие конфиденциальной информации;

• нельзя гарантировать абсолютную защищенность информации.

Пассивный метод заключается в уменьшении мощности самого излучаемого сигнала. Осуществление подобного метода заключается в изоляции излучающих проводников, устройств, а также периметра помещения специальными материалами поглощающими ЭМП, в отношении проводных линий – установка фильтров.

Активные методы основаны на увеличении уровня шума путем применения генераторов пространственного зашумления. Данные устройства, как правило, формируют широкополосную помеху во всем диапазоне частот. Регулировка в большинстве моделей осуществляется только по общему уровню сигнала, за редким исключением присутствует возможность корректировки частотной характеристики на низких, средних и высоких частотах.

С точки зрения заключения договора на аттестацию ОИ применение САЗ самый удобный и простой вариант, а иногда и единственный (если организация арендует 1-2 помещения и расстояние до границы КЗ 1 м).

Наиболее популярные модели САЗ по каналу ПЭМИН приведены. приведен скан сертификата ФСТЭК России на САЗ «Соната-Р3.1».

Рисунок 1. Средство активной защиты от утечек за счет ПЭМИН «Соната-Р3.1»

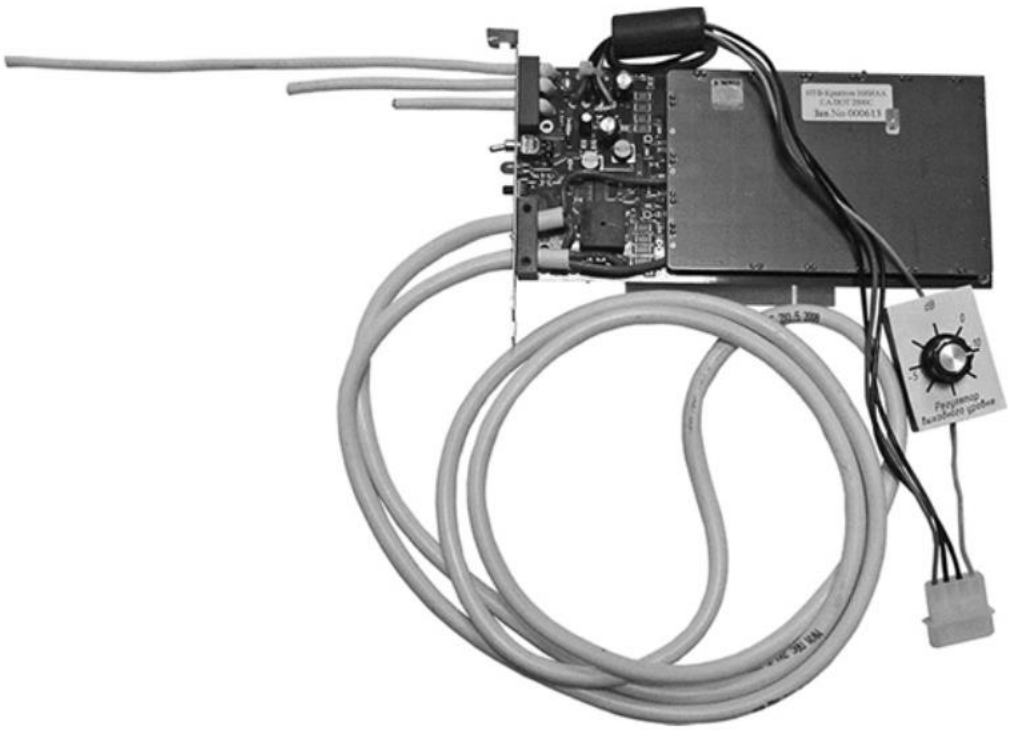


Рисунок 2. Средство активной защиты информации от утечек за счет ПЭМИН «Салют 2000С»

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3539

Выдан 24 марта 2016 г.
Действителен до 24 марта 2019 г.

Настоящий сертификат удостоверяет, что **средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «Соната-Р3.1»**, разработанное и производимое ООО «Анна» в соответствии с техническими условиями ЮДИН.665820.015 ТУ, является средством активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок типа «А» и «Б», соответствует требованиям документа «Требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, 2014) – по **2** классу защиты, может применяться в выделенных помещениях до **1** категории включительно.

Рисунок 3. Сертификат соответствия ФСТЭК России на СЗИ «Соната-Р3.1»

Исходя из графика спектров помех можно сделать вывод, что во всем диапазоне частот помехи не обладают равномерным спектром. Вследствие чего, при проведении измерений, сигналы ПЭМИ могут оказаться на частотах, соответствующих «провалам» в спектре помехи, что поставит под вопрос защищенность объекта. Проблема в том, что с точки зрения требований по сертификации САЗ по каналу ПЭМИН, оценивается только спектральная плотность мощности, причем в достаточно широкой полосе, а то, как ведет себя спектр помехи в данной полосе это уже будет видно на практике (для примера приведем характеристики САЗ «Соната-Р2», табл. 2–4).

Таблица 2

Спектральная плотность напряженности электрической составляющей ЭМП «Соната-Р2», не менее

Диапазон частот, МГц	Вертикальная поляризация, дБ		Горизонтальная поляризация, дБ	
	Без дополнительной антенны	С дополнительной антенной	Без дополнительной антенны	С дополнительной антенной
от 0,01 до 0,15	50	80	50	80
от 0,15 до 1	45	70	40	70
от 1 до 5	45	60	40	55
от 5 до 30	45	60	40	50
от 30 до 100	40	50	40	50
от 100 до 1000	30	30	30	30
от 1000 до 2000	30	30	30	30

Таблица 3

Спектральная плотность напряженности магнитной составляющей ЭМП «Соната-Р2», не менее

Диапазон частот, МГц	Без дополнительной антенны, дБ	С дополнительной антенной, дБ
от 0,01 до 0,15	30	30
от 0,15 до 4	35	35
от 4 до 10	40	40
от 10 до 30	30	35

Таблица 4

Спектральная плотность напряжения помех в линиях электропитания и заземления «Соната-Р2», не менее

Диапазон частот, МГц	Без дополнительной антенны, дБ	С дополнительной антенной, дБ
от 0,01 до 0,04	25	25
от 0,04 до 10	35	35
от 10 до 100	35	45
от 100 до 600	25	25
от 600 до 1000	15	15

Пассивные методы защиты информации от утечки по каналам ПЭМИН возможно реализовать следующими путями:

- уменьшение уровня информативного сигнала за счет экранирования помещения (что практически невозможно, гарантию может дать только специализированная экран камера, которая применяется для лабораторных исследований источников радиосигналов).
- если в процессе анализа выявлено, что ТКУИ возникает только за счет наводок на линии электропитания, то возможно применение сетевых подавляющих фильтров (рисунок 3).

Рисунок 3. Фильтр сетевой помехоподавляющий ЛФС-10-1Ф

Фильтр сетевой помехоподавляющий ЛФС-10-1Ф предназначен для защиты информации, обрабатываемой техническими средствами и системами и содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа от утечки по каналам побочных электромагнитных наводок на линии электропитания напряжением 220 В с частотой 50 Гц

«ЛФС-10-1Ф» соответствует: типу – пассивные средства защиты информации от утечки за счет побочных электромагнитных наводок на линии электропитания.

«ЛФС-10-1Ф» соответствует документу «Требования к пассивным средствам защиты информации от побочных электромагнитных наводок на линии электропитания» (ФСТЭК России, 2015), – по 1 классу защиты.

Отметим, что на практике чаще всего в случае невыполнения норм защищенности применяются средства активной защиты – генераторы электромагнитного шума, которые также создают наведенную помеху на линии и токоведущие коммуникации.

Практическая часть.

Вопросы для самопроверки:

11) Опишите самый простой и удобный способ на аттестацию ОИ при применении САЗ.

12) По какому классу защиты соответствует ЛФС-10-1Ф?

13) Что такое активная защита САЗ?

14) Что такое пассивная защита САЗ?

15) Какими методами по защите информации от утечек ПЭМИН возможно реализовать пассивные меры защиты?

Практические задания:

4) По вашему мнению, является ли допустимым использование одновременно и пассивных и активных мер защиты? Если возможно, в подробности расскажите почему?

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Введение. Основные понятия теории компьютерной безопасности	***Подготовка докладов и презентаций по темам:*** Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников. ***Самостоятельное изучение темы*** (тематика определяется преподавателем
2.	Анализ угроз информационной безопасности для компьютерных си-	***Подготовка докладов и презентаций по темам:*** Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и

	стем	функционального назначения. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.
3	Основные уровни защиты информации в компьютерных системах	***Подготовка докладов и презентаций по темам:*** Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС. Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA. Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков.
4	Основные положения формальной теории защиты информации	***Подготовка докладов и презентаций по темам:*** Перечень основных документов ФСТЭК России по вопросам защиты информации. Система разграничения доступа (СРД) и её функции. Средства для СРД. Реализация СРД. ***Самостоятельное изучение темы*** (тематика определяется преподавателем
5	Формальные модели безопасности	***Подготовка докладов и презентаций по темам:*** Построение модели нарушителя безопасности АС. Уровни возможностей, предоставляемые нарушителям штатными средствами АС и СВТ. Базовая модель угроз ИСПДн. Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant.
6	Концептуальные положения системы ме-	***Подготовка докладов и презентаций по темам:***

	неджмента информационной безопасности применительно к компьютерным системам	Лицензирование и сертификация в области защиты информации. Комплексные системы защиты информации. Аттестация АС по требованиям безопасности информации. ***Самостоятельное изучение темы*** (тематика определяется преподавателем
7	Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной информации	***Подготовка докладов и презентаций по темам:*** Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU). Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации и механизмы управления. Выбор способа постановки задачи. Методы построения защищённых АС. Принципы проектирования. Структурный принцип и принцип модульного проектирования. Три основных конструкции для проектирования. Преимущества использования модульного принципа. ***Самостоятельное изучение темы*** (тематика определяется преподавателем **Письменная работа** Предложения руководителю для принятия решения в рамках КБ по обеспечению функционирования объекта информатизации.

5. Указания по проведению контрольных работ для обучающихся очной формы обучения

5.1. Требования к структуре.

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части).

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы: «раскрыть», «определить», «установить», «показать», «выявить» и т.д.

3. Основная часть работы включает 2 - 4 вопроса, каждый из которых посвящается решению задач, сформулированных во введении, и заканчивается констатацией итогов.

4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).

5. Необходимо давать ссылки на используемую литературу.

6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

7. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению.

Объём контрольной работы – … страниц формата А4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основная литература:

1.Гагарина Л.Г., Федоров А.Р., Федоров П.А. Введение в архитектуру программного обеспечения: Учебное пособие - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 320 с. ISBN 978-5-8199-0649-1. / ЭБС «Знаниум» http://znanium.com/bookread2.php?book=542665

2.Астапчук В.А., Терещенко П.В. Архитектура корпоративных информационных систем – Новосиб.: НГТУ, 2015. - 75 с.: ISBN 978-5-7782-2698-2. / ЭБС «Знаниум» http://znanium.com/bookread2.php?book=546624

Дополнительная литература:

3.Царев Р.Ю., Прокопенко А.В., Князьков А.Н. Программные и аппаратные средства информатики - Краснояр.: СФУ, 2015. - 160 с. ISBN 978-5-7638-3187-0 / ЭБС «Знаниум» http://znanium.com/bookread2.php?book=550017

4.Дворовенко, О. В. Информационно-аналитические продукты и услуги: практикум по направлению подготовки 51.03.06 «Библиотечно-информационная деятельность», профиль подготовки «Информационно-аналитическая деятельность», квалификация (степень) выпускника: «бакалавр» : учебное пособие / О. В. Дворовенко. — Кемерово : КемГИК, 2021. — 54 с. — ISBN 978-5-8154-0604-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/250628 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей. ЭБС Лань (lanbook.com)

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Интернет-ресурсы:

1. 1. www.biblioclub.ru - Универсальная библиотека онлайн.
2. www.rucont.ru - ЭБС «Руконт».
3. http://www.academy.it.ru/ – академия АЙТИ.
4. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
5. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации
6. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности
7. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1.Электронные ресурсы образовательной среды Университета.
2.Информационно-справочные системы: Консультант+; Гарант.