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.ДВ.05.01 ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ ВЫЯВЛЕНИЯ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

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: Вихров А.П. Рабочая программа дисциплины (модуля): Инструментальные методы выявления технических каналов утечки информации. – 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	№5 от 11.04.2023г.			

2

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины является формирование у студентов базовых знаний в области методов и средств контроля эффективности защиты информации от утечки по техническим каналам и навыков практической работы с изучаемыми техническими средствами.

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

Профессиональные компетенции:

- ПК-2: Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном исполнении.
- 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.

Задачами дисциплины являются**:**

1. Изучение физических основ формирования технических каналов утечки информации (ТКУИ).
2. Изучение возможных ТКУИ на объектах защиты и инструментальных средств их измерения и определения.
3. Формирование у студентов практических навыков измерения основных характеристик технических каналов утечки информации.
4. Формирование у студентов практических навыков по выбору и разработке систем и технологий обеспечения информационной безопасности.
5. Обучение разработкам планов и программ проведения научных исследований и технических разработок, подготовке отдельных заданий для исполнителей, проведению научно-исследовательских работ по заданной тематике.
6. Обеспечение участия в работах по созданию, изготовлению, монтажу, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформлением технических заданий на проектирование, осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированной ИАС.
- ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда

Необходимые умения:

- ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии защиты автоматизированной ИАД с разработкой

проектной документации и комплексной оценкой эффективности применения автоматизированной ИАС.

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

Необходимые знания:

- ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем, методы проектирования, критерии и показатели эффективности автоматизированной ИАС.

- 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 относится к дисциплинам по выбору 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: “Специальные разделы физики”, “Технологии обеспечения информационной безопасности объектов”, “Методы и средства обеспечения безопасного доступа к информационным ресурсам” и компетенциях: УК-2, 4; ОПК-2; ПК-2, 3.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при дальнейшем изучении дисциплин общенаучного цикла «Компьютерное моделирование информационных процессов и технологий», «Комплексная проверка информационной безопасности» и для написания магистерской диссертации..

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

Общая трудоемкость дисциплины для обучающихся очной формы составляет 2 зачетных единицы, 72 часа.

Таблица1

Виды занятий	**Всего часов**	**Семестр 3**	**Семестр …**	**Семестр …**	**Семестр …**
Общая трудоемкость	**72**	**72**			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**46**	**46**			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	8	8			
Практическая подготовка	**4**	**4**			
Другие виды контактной работы*	**6**	**6**			
Самостоятельная работа	**26**	**26**			
Курсовые работы (проекты)	**-**	**-**			
Расчетно-графические работы	**-**	**-**			
Контрольная работа, домашнее задание	**+**	**+**			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	**-**	**-**			
Вид итогового контроля	Зачет	Зачет			

* 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.	Практ. занятия, час.	Лабораторные работы, час.	Занятия в интерактивной форме, час.	Практическая погото вка ,час	Код компетенций
1	2	3	4	5	6	7
Тема 1. Основные сведения о каналах утечки информации. Средства обнаружения и контроля эффективности защищенности информации	4	4	2	2	1	ПК-2
Тема 2. Методика проведения специальных исследований в области защиты речевой информации	4	4	2	2	1	ПК-2
Тема 3. Методика проведения специальных исследований в области акустоэлектрических преобразований	4	4	2	2	1	ПК-3
Тема 4. Методика проведения специальных исследований в области побочных электромагнитных излучений	4	4	2	4	1	ПК-2,3
Итого	**16**	**16**	**8**	**10**	**4**	

4.2. Содержание тем дисциплины

Тема 1. Основные сведения о каналах утечки информации. Средства обнаружения и контроля эффективности защищенности информации

Каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации: электромагнитные, электрические, параметрические и вибрационные каналы.

Каналы утечки речевой информации: акустические, виброакустические, акустоэлектронные, оптикоэлектронные и параметрические каналы.

Каналы утечки информации при ее передаче по каналам связи. Технические каналы утечки видовой информации. Технические каналы утечки информации, возникающие при работе вычислительной техники за счет ПЭМИН.

Индикаторы электромагнитных излучений, радиочастотомеры, сканирующие приемники, высокоскоростные поисковые приемники, селективные микровольтметры, анализаторы спектра.

Нелинейные локаторы, металлодетекторы, эндоскопы, тепловизионные локаторы.

Автоматизированные поисковые комплексы, специализированные поисковые программно-аппаратные комплексы.

Тема 2. Методика проведения специальных исследований в области защиты речевой информации

Методика проведения измерений акустического сигнала за пределами ограждающих конструкций: пол, потолок, стены, вентиляционные шахты, двери. Требования к источнику акустического сигнала. Требования к измерительной аппаратуре.

Методика проведения измерений вибрационного сигнала на системах отопления и оконных стеклах. Требования к источнику акустического сигнала. Требования к измерительной аппаратуре.

Тема 3. Методика проведения специальных исследований в области акустоэлектрических преобразований

Методика проведения специальных исследований в области акустоэлектрических преобразований во вторичных технических средствах и системах и в бытовой аппаратуре.

Требования к источнику акустического сигнала и к техническим средствам измерения.

Тема 4. Методика проведения специальных исследований в области побочных электромагнитных излучений

Особенности спектра цифровых сигналов, излучаемых подсистемами вычислительной техники. Тестовые сигналы. Методика проведения расчета уровня ПЭМИ на границе контролируемой зоны.

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

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

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

Структура фонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Инструментальные методы выявления технических каналов утечки информации» приведена в Приложении 1.

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

Основная литература:

1.Техническая защита информации : учебное пособие / А. С. Раков, О. Н. Маслов, О. Ю. Губарева [и др.]. — Самара : ПГУТИ, 2020. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/255575 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2018. — 168 с. — ISBN 978-5-4383-0161-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103203 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3.Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110328 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

4. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2012. — 374 с. — Текст : электронный // Лань : электронно-библиотечная система. —

URL: https://e.lanbook.com/book/11381 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., и др..Технические средства и методы защиты информации. Учебное пособие Под ред. А.П.Зайцева и А.А.Шелупанова. 4-е издание исправленное и дополненное. - М.: Горячая линия – Телеком, 2012.- 616с..
2. Основы теории передачи информации: Учебное пособие - М.:, Литвинская О.С. , КНОРУС, 2010. ISBN 978-5-406-00049-6
3. Торокин А.А. Инженерно-техническая защиты информации: Учебное пособие. М.: Гелиос АРВ, 2008.
4. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации: Учебное пособие. М.: «Академия», 200
5. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. Учебное пособие. –М.: Горячая линия – Телеком, 2005.
6. ГОСТ 12.1.050-86 «Методы измерения шума на рабочих местах».
7. ГОСТ 29216-91 «Совместимость технических средств электромагнитная. Радиопомехи индустриальные от оборудования информационной техники. Нормы и методы испытаний.»
8. ГОСТ 22505-83 «Радиопомехи индустриальные от приемников телевизионных и приемников радиовещательных частотно-модулированных сигналов в диапазоне УКВ. Нормы и методы измерений.»
9. Инструкция по эксплуатации измерителя шума и вибрации ВШВ-003-М3.
6. Инструкция по эксплуатации скоростного поискового приемника радиосигналов «Скорпион», БНТИ-ТСС, Москва, 2006.
10. Руководство пользователя комплекса «Омега», ОАО НОВО, Москва, 2005.

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

Интернет-ресурсы:

1. http://www.biblioclub.ru
2. http://znanium.com
3. www.rucont.ru

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

Методические указания для обучающихся, по освоению дисциплины, приведены в Приложении 2.

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

- **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.

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения занятий в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже Windows XP; офисные программы MS Office 7;
- контрольно-измерительная аппаратура (комплекс «Омега»);
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Практические занятия целесообразно проводить в специализированной учебной лаборатории кафедры информационной безопасности с использованием имеющихся технических средств:

1. Имитатор многофункциональный ИМФ-2;
2. Многофункциональный комплекс радиоконтроля «Омега»;
3. Измеритель шума и вибраций ВШВ-003-М3;
4. Поисковый приемник радиосигналов «Скорпион».
5. Селективные микровольтметры;
6. Анализатор спектра;

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.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ ВЫЯВЛЕНИЯ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

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	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1	2	3	4	5	6	7
1.	ПК-2	Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном исполнении.	Тема:1, 2, 4	ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформлением технических заданий на проектирование, осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированной ИАС.	ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии защиты автоматизированной ИАД с разработкой проектной документации и комплексной оценкой эффективности применения автоматизированной ИАС.	ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем, методы проектирования, критерии и показатели эффективности автоматизированной ИАС.
2.	ПК-3	Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-	Тема:1, 2	ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития,	ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать	ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1	2	3	4	5	6	7
		обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности.		области научного знания и рынка труда.	методическую помощь в их выполнении.	теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструменты, оценивающие сформированность компетенции	Этапы и показатель оценивания компетенции	Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания
ПК-2,3	***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.***
ПК-2,3	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.
ПК-2,3	Лабораторная работа	А) полностью сформирована (компетенция освоена на <u>высоком</u>	Например: 1. Оформление в соответствии с требованиями (1 балл). 2. Выбор методов измерений и

		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	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.

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 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.

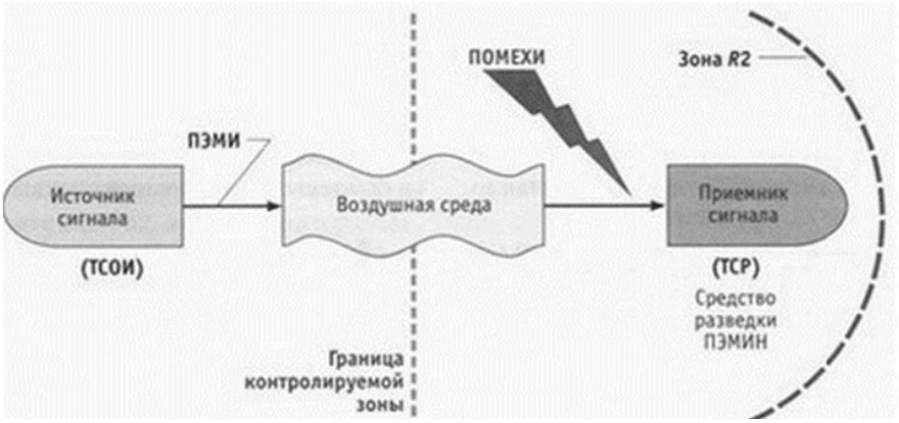

Рисунок 1. Схема ТКУИ за счет ПЭМИ

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

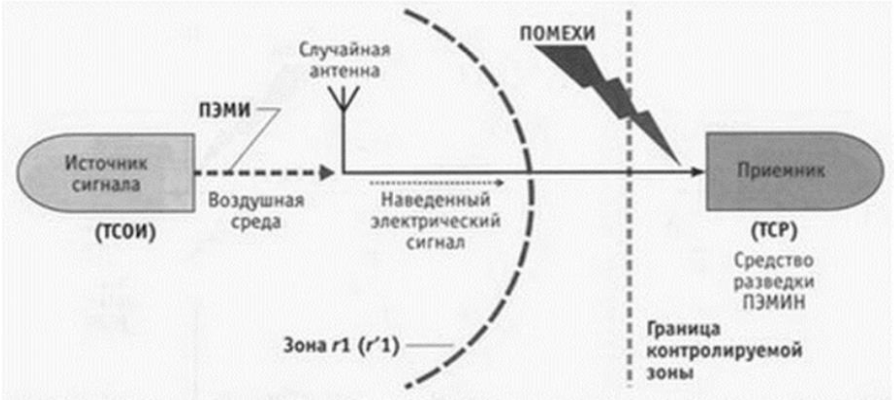

Рисунок 2. Схема ТКУИ за счет ПЭМИН

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:

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 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

Вопросы, выносимые на самостоятельное изучение:

1. Структурное моделирование.
2. Модель белого ящика и ее практическое использование
3. Что такое структурная схема и чем граф отличается от сети.
4. Модель черного ящика и ее практическое использование
5. Построить формальную модель педагогического процесса в вузе.
6. Операция декомпозиция и ее практическое использование при моделировании информационных процессов.
7. Временные структурные модели в экономике и промышленности.
8. Структурная схема системы.
9. Гармонический осциллятор- содержательная и математическая постановка задачи.
10. Модель конкуренции двух популяций.
11. Понятия устойчивости и неустойчивости стационарных состояний.
12. Понятие множественности стационарных состояний в процессах теплопередачи.
13. Модель Мальтуса и результаты ее анализа.
14. Модель спроса и предложения.
15. Статистический анализ простейших конструкций.
16. Причины возможной неадекватности математической модели.
17. Каким требованиям должна удолетворять корректная модель.
18. Выполните содержательную, концептуальную и математическую постановку задачи обеспечения информационной безопасности предприятия.
19. Проверка адекватности модели.
20. Этапы разработки программного обеспечения для анализа математичской модели
21. Язык формального описания алгоритмов.

ЗАДАНИЕ № 2

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.

4. Изучить теоретическую часть Задания №4.
5. Выполнить практическую часть Задания №4:
   а) ответить на вопросы для самопроверки;
   б) выполнить практические задания.
6. 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»

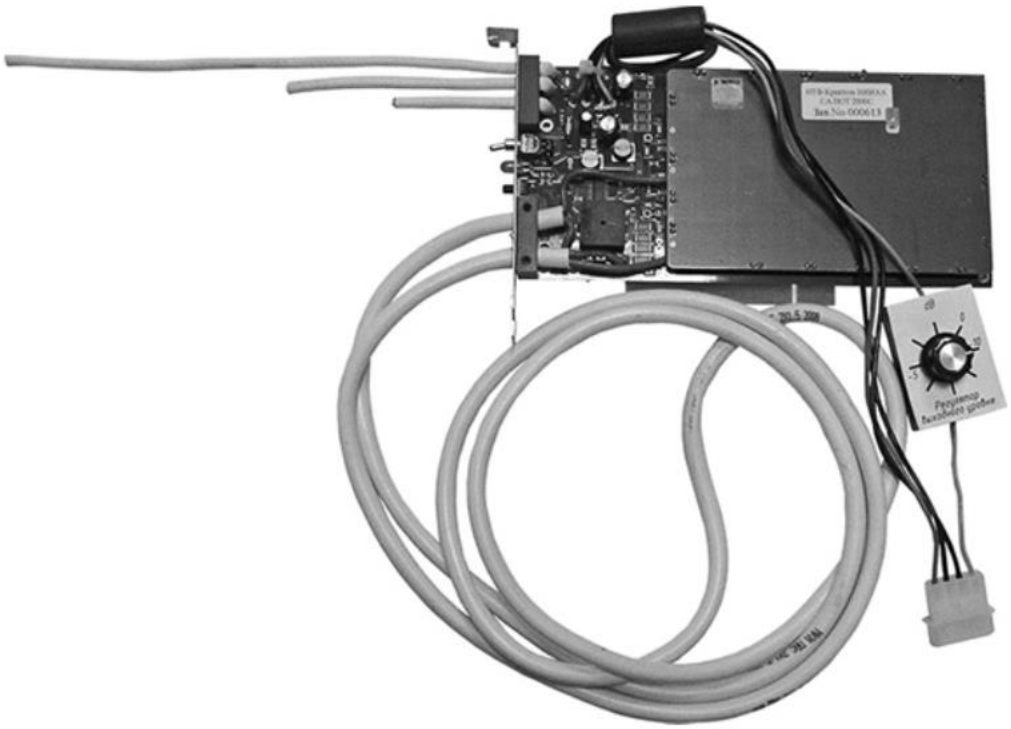

Рисунок 2. Средство активной защиты информации от утечек за счет ПЭМИН «Салют 2000С»

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:

1) Опишите самый простой и удобный способ на аттестацию ОИ при применении САЗ.
2) По какому классу защиты соответствует ЛФС-10-1Ф?
3) Что такое активная защита САЗ?
4) Что такое пассивная защита САЗ?
5) Какими методами по защите информации от утечек ПЭМИН возможно реализовать пассивные меры защиты?

Практические задания:

1) По вашему мнению, является ли допустимым использование одновременно и пассивных и активных мер защиты? Если возможно, в подробности расскажите почему?

Примерная тематика докладов в форме презентаций:

1. Физические основы формирования технических каналов утечки информации.
2. Акустический канал утечки информации и средства его измерения.
3. Акусто-электрический канал утечки информации и средства его измерения.
4. Акусто-вибрационный канал утечки информации и средства его измерения.
5. Канал утечки информации, связанный с высоко-частотным навязыванием, и средства его измерения..
6. Канал утечки информации, связанный с высоко-частотным облучением, и средства его измерения..
7. Каналы утечки информации, связанные с ПЭМИН, и средства его измерения.
8. Параметрические каналы утечки информации и средства их измерения.
9. Порядок аттестации по требованиям безопасности конфиденциальной информации объекта вычислительной техники.
10. Порядок аттестации по требованиям безопасности конфиденциальной информации защищаемого помещения.
11. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности. Основы обеспечения безопасности информации в компьютерных системах.
12. 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.
13. Проектирование архитектуры системы защиты информации выбранного объекта и оценка его уровня защищённости.
14. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников.
15. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации.
16. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию.
17. Направления повышения эффективности существующей системы защиты и методика применения средств защиты информации на выбранных объектах исследования.

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

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

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

21. Компьютерная преступность в экономических областях.

22. Компьютерные вирусы в современных информационных системах.

23. Информационные угрозы современным экономическим объектам.

24. Безопасность информации в коммерческой деятельности.

25. Становление и развитие промышленного шпионажа.

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

27. Информационные угрозы современным экономическим объектам.

28. Безопасность информации в коммерческой деятельности.

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

Формой контроля знаний по дисциплине «Инструментальные методы выявления технических каналов утечки информации» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

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
1	2	3	5	5	6	7
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-2,3	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	ПК-2,3	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.***

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
1	2	3	5	5	6	7
						Хорошо - от 70%. Отлично – от 90%
Проводится в сроки, установленные графиком образовательного процесса	зачет	ПК-2,3	3 вопроса	зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачета	Критерии оценки: **«Зачтено»:** • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на семинарских занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. **«Не зачтено»**: демонстрирует частичные знания по темам дисциплин;

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
1	2	3	5	5	6	7
						• незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на семинарских 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.

4.1. Типовые вопросы, выносимые на тестирование

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

1. 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

2. Требование безопасности повторного использования объектов противоречит:
инкапсуляции +
наследованию
полиморфизму

3. 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

4. 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

5. Уровни модели TCP/IP, по возрастанию:
канальный, сетевой, транспортный, прикладной +
транспортный, канальный, сетевой, прикладной
канальный, транспортный, сетевой, прикладной
прикладной, сетевой, транспортный, канальный

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

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

8. Что входит в функции систем мониторинга:
выявление состояния систем
установка отношений между объектами

установка соответствия правил и обязанностей
все варианты верны +

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

10. Дублирование сообщений является угрозой:
доступности
конфиденциальности
целостности +

11. Какие существуют методы оценки качества КСИБ:
метод оценки уязвимости Хоффмана +
экспертная оценка +
сигнатурный метод
качественный метод.

12. Самыми опасными источниками внутренних угроз являются:
некомпетентные руководители +
обиженные сотрудники
любопытные администраторы

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

14. 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

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

16. 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.

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

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

19. 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 +

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

21. Требование безопасности повторного использования объектов противоречит:
инкапсуляции +
наследованию
полиморфизму

22. 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

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

24. Дублирование сообщений является угрозой:
доступности

конфиденциальности
целостности +

25. Самыми опасными источниками внутренних угроз являются:
некомпетентные руководители +
обиженные сотрудники
любопытные администраторы

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

27. 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

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

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

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

31. 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 +

4.2 Типовые вопросы, выносимые на зачет

1. ТКУИ, связанные с акустическими преобразованиями.
2. Акустический канал утечки информации.
3. Организационные основы защиты информации: технологические и правовые составляющие.

4. Физические основы формирования технических каналов утечки информации.
5. Порядок аттестации по требованиям безопасности конфиденциальной информации объекта вычислительной техники.
6. Порядок аттестации по требованиям безопасности конфиденциальной информации защищаемого помещения.
7. Каналы утечки информации, обрабатываемой техническими средствами.
8. Акустические и виброакустические каналы утечки речевой информации.
9. Акустоэлектронные, оптикоэлектронные и параметрические каналы утечки речевой информации.
10. Каналы утечки информации при ее передаче по каналам связи.
11. Технические каналы утечки видовой информации.
12. Технические каналы утечки информации, возникающие при работе вычислительной техники за счет ПЭМИН.
13. Структурная схема и принцип работы индикаторов электромагнитных излучений.
14. Структурная схема и принцип работы радиочастотомера.
15. Структурная схема и принцип работы сканирующего приемника.
16. Структурная схема и принцип работы анализатора спектра.
17. Структурная схема и принцип работы нелинейного локатора.
18. Структурная схема и принцип работы металлодетекторы.
19. Методика проведения измерений акустического сигнала за пределами ограждающих конструкций.
20. Требования к источнику акустического сигнала при проведении измерений акустического сигнала за пределами ограждающих конструкций.
21. Требования к измерительной аппаратуре при проведении измерений акустического сигнала за пределами ограждающих конструкций.
22. Методика проведения измерений вибрационного сигнала на системах отопления и оконных стеклах.
23. Требования к источнику акустического сигнала при проведении измерений вибрационного сигнала.
24. Требования к измерительной аппаратуре при проведении измерений вибрационного сигнала.
25. Методика проведения специальных исследований в области акустоэлектрических преобразований во вторичных технических средствах и системах и в бытовой аппаратуре.
26. Требования к источнику акустического сигнала и к техническим средствам измерения при проведении специальных исследований в области акустоэлектрических преобразований.
27. Особенности спектра цифровых синалов, излучаемых подсистемами вычислительной техники.
28. Тестовые сигналы для проведения специальных исследований.

29. Методика проведения расчета уровня ПЭМИ на границе контролируемой зоны.
30. Методика проведения измерений уровня ПЭМИ на границе контролируемой зоны.

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 ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ ВЫЯВЛЕНИЯ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

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:

Сформировать у студентов базовые знания в области методов и средств контроля эффективности защиты информации от утечки по техническим каналам и навыков практической работы с изучаемыми техническими средствами.

Задачи дисциплины:

- Изучение физических основ формирования технических каналов утечки информации (ТКУИ).
- Изучение возможных ТКУИ на объектах защиты и инструментальных средств их измерения и определения.
- Формирование у студентов практических навыков измерения основных характеристик технических каналов утечки информации.
- Формирование у студентов практических навыков по выбору и разработке систем и технологий обеспечения информационной безопасности.
- Обучение разработкам планов и программ проведения научных исследований и технических разработок, подготовке отдельных заданий для исполнителей, проведению научно-исследовательских работ по заданной тематике.
- Обеспечение участия в работах по созданию, изготовлению, монтажу, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности.

2. Указания по проведению практических занятий

Тема 1. Основные сведения о каналах утечки информации. Средства обнаружения и контроля эффективности защищенности информации

Практическое занятие 1.

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

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия: Основные сведения о каналах утечки информации.

Форма проведения: разбор конкретных ситуаций.

Учебные вопросы.

1. Выделение акустических каналов утечки информации в учебной аудитории.
2. Выделение вибрационных каналов утечки информации в учебной аудитории.

Продолжительность занятия – 1 ч.

Тема 1. Основные сведения о каналах утечки информации. Средства обнаружения и контроля эффективности защищенности информации

Практическое занятие 2.

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

Образовательные технологии: беседа.

Тема и содержание практического занятия: Средства обнаружения и контроля эффективности защищенности информации.

Форма проведения: разбор конкретных ситуаций

Учебные вопросы.

1. Анализ структурной схемы поискового приемника «Скорпион»
2. Анализ технических характеристик поискового приемника «Скорпион»

Продолжительность занятия – 1 ч.

Тема 1. Основные сведения о каналах утечки информации. Средства обнаружения и контроля эффективности защищенности информации

Практическое занятие 3.

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

Образовательные технологии: *практическая работа в группах*

Тема и содержание практического занятия: Средства обнаружения и контроля эффективности защищенности информации.

Форма проведения: разбор конкретных ситуаций

Учебные вопросы.

1. Анализ структурной схемы комплекса радиоконтроля «Омега»

2. Анализ технических характеристик комплекса радиоконтроля «Омега»

Продолжительность занятия – 1 ч.

Тема 1. Основные сведения о каналах утечки информации. Средства обнаружения и контроля эффективности защищенности информации

Практическое занятие 4.

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

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия: Средства обнаружения и контроля эффективности защищенности информации.

Форма проведения: разбор конкретных ситуаций с применением современных технических средств

Учебные вопросы.

2. Анализ структурной схемы измерителя шума и вибраций ВШВ-3-М3.
3. Методика измерения уровня интенсивности акустических сигналов.
4. Методика измерения уровня вибрационных сигналов.

Продолжительность занятия – 1 ч.

Тема 2. Методика проведения специальных исследований в области защиты речевой информации

Практическое занятие 5

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

Образовательные технологии: беседа.

Тема и содержание практического занятия: Методика проведения специальных исследований в области защиты речевой информации.

Форма проведения: разбор конкретных ситуаций с применением современных технических средств

Учебные вопросы.

1. Анализ методики измерения акустических сигналов на границе контролируемой зоны.
2. Обработка экспериментальных данных и составление отчета об испытаниях.

Продолжительность занятия – 1 ч.

Тема 2. Методика проведения специальных исследований в области защиты речевой информации

Практическое занятие 6.

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

Образовательные технологии: *практическая работа в группах.*

Тема и содержание практического занятия: Методика проведения специальных исследований в области защиты речевой информации.

Форма проведения: разбор конкретных ситуаций с применением современных технических средств

Учебные вопросы

1. Анализ методики измерения вибрационных сигналов на ограждающих конструкциях.
2. Обработка экспериментальных данных и составление отчета об испытаниях.

Продолжительность занятия – 1 ч.

Тема 3. Методика проведения специальных исследований в области акустоэлектрических преобразований

Практическое занятие 7

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

Образовательные технологии: *беседа.*

Тема и содержание практического занятия: Методика проведения специальных исследований в области защиты речевой информации.

Форма проведения: разбор конкретных ситуаций с применением современных технических средств

Учебные вопросы

1. Формирование акустического сигнала с заданным спектром с помощью программы Audacity.
2. Калибровка измерителя шума и вибраций ВШВ-3-М3.
3. Измерение спектральных составляющих акустического сигнала на октавных частотах.

Продолжительность занятия – 1 ч.

Тема 3. Методика проведения специальных исследований в области акустоэлектрических преобразований

Практическое занятие 8.

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

Образовательные технологии: *беседа.*

Тема и содержание практического занятия: Методика проведения специальных исследований в области защиты речевой информации

Форма проведения: разбор конкретных ситуаций с применением современных технических средств

Учебные вопросы.

1. Измерение уровня акустического сигнала за пределами ограждающей конструкции (стены).
2. Измерение уровня акустического сигнала за пределами дверного проема.

Продолжительность занятия – 1 ч.

Тема 3. Методика проведения специальных исследований в области акустоэлектрических преобразований

Практическое занятие 9

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

Тема и содержание практического занятия: Методика проведения специальных исследований в области защиты речевой информации.

Форма проведения: разбор конкретных ситуаций с применением современных технических средств

Учебные вопросы.

1. Измерение уровня вибрационного сигнала на внутреннем стекле оконного проема.
2. Измерение уровня вибрационного сигнала на трубах системы центрального отопления.

Продолжительность занятия – 2 ч.

Тема 3. Методика проведения специальных исследований в области акустоэлектрических преобразований

Практическое занятие 10.

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

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия: Методика проведения специальных исследований в области акустоэлектрических преобразований.

Форма проведения: разбор конкретных ситуаций с применением современных технических средств

Учебные вопросы.

1. Рассмотрение численных примеров акустоэлектрического преобразования в гетеродинах телевизионных и радиовещательных приемников.
2. Анализ примера акустоэлектрического преобразования в динамиках систем звукоусиления и анализ методики измерения опасного сигнала.

Продолжительность занятия – 2 ч.

Тема 4. Методика проведения специальных исследований в области побочных электромагнитных излучений

Практическое занятие 11.

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

Образовательные технологии: *беседа*

Тема и содержание практического занятия: Методика проведения специальных исследований в области акустоэлектрических преобразований.

Форма проведения: разбор конкретных ситуаций с применением современных технических средств

1. Анализ методики измерения опасных сигналов в силовых цепях бытовой техники.
2. Анализ формирования опасных сигналов в системах телефонной сиязи и методика их измерения.

Продолжительность занятия – 2 ч.

Тема 4. Методика проведения специальных исследований в области побочных электромагнитных излучений

Практическое занятие 12

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

Образовательные технологии: *практическая работа в группах.*

Тема и содержание практического занятия: Специальные исследования в области ПЭМИ.

Форма проведения: разбор конкретных ситуаций с применением современных технических средств

Учебные вопросы.

1. Анализ временных и спектральных характеристик сигнала, излучаемого подсистемой отображения информации компьютера.

2. Анализ временных и спектральных характеристик различных тестовых сигналов.

Продолжительность занятия – 2 ч.

3. Указания по проведению лабораторного практикума

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-4 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.

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 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.

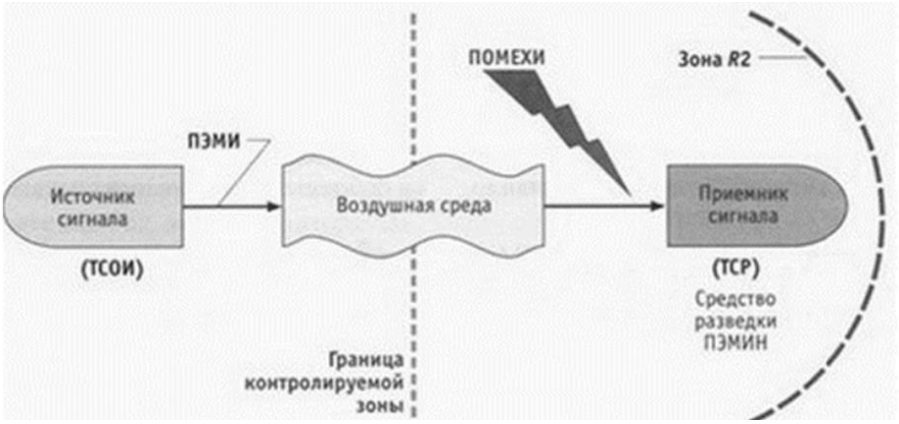

Рисунок 1. Схема ТКУИ за счет ПЭМИ

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

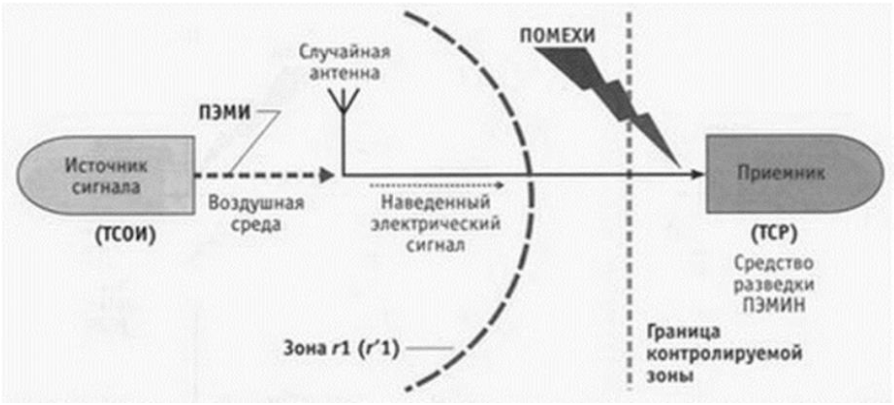

Рисунок 2. Схема ТКУИ за счет ПЭМИН

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:

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 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

Лабораторная работа № 2. Анализ угроз информационной безопасности

Цель работы: Изучить и научиться выполнять анализ условий и факторов воздействующих 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.

Задание.

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	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:

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.

Продолжительность практического занятия-4 часа

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Основные сведения о каналах утечки информации. Средства обнаружения и контроля эффективности защищенности информации	***Подготовка докладов по темам:*** Физические основы формирования технических каналов утечки информации (ТКУИ) .Акустический канал утечки информации. Комплексные системы защиты информации *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
2.	Методика проведения специальных исследований в области защиты речевой информации	***Подготовка докладов по темам:*** Порядок аттестации по требованиям безопасности конфиденциальной информации объекта вычислительной техники. Порядок аттестации по требованиям безопасности конфиденциальной информации защищаемого помещения. Аттестация объектов информатизации. Виды защиты информации. *Подготовка рефератов, письменная работа,*

		самостоятельное изучение тем.
3	Методика проведения специальных исследований в области акустоэлектрических преобразований	***Подготовка докладов по темам:*** Принципы и методы организационной защиты информации. Методы и средства обнаружения уязвимостей в корпоративных компьютерных сетях. Лицензирование и сертификация в области защиты информации. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
4	Методика проведения специальных исследований в области побочных электромагнитных излучений	***Подготовка докладов по темам:*** Принципы организации информационных систем в соответствии с требованиями по защите информации. Методы программно-аппаратной защиты информации. Способы и средства защиты информации от утечки по техническим каналам. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*

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.

Основная литература:

1.Техническая защита информации : учебное пособие / А. С. Раков, О. Н. Маслов, О. Ю. Губарева [и др.]. — Самара : ПГУТИ, 2020. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/255575 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2018. — 168 с. — ISBN 978-5-4383-0161-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103203 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3.Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110328 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

4. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2012. — 374 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/11381 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., и др..Технические средства и методы защиты информации. Учебное пособие Под ред. А.П.Зайцева и А.А.Шелупанова. 4-е издание исправленное и дополненное. - М.: Горячая линия – Телеком, 2012.- 616с..

2. Основы теории передачи информации: Учебное пособие - М.:, Литвинская О.С. , КНОРУС, 2010. ISBN 978-5-406-00049-6

3. Торокин А.А. Инженерно-техническая защиты информации: Учебное пособие. М.: Гелиос АРВ, 2008.

4. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации: Учебное пособие. М.: «Академия», 200
5. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. Учебное пособие. –М.: Горячая линия – Телеком, 2005.
6. ГОСТ 12.1.050-86 «Методы измерения шума на рабочих местах».
7. ГОСТ 29216-91 «Совместимость технических средств электромагнитная. Радиопомехи индустриальные от оборудования информационной техники. Нормы и методы испытаний.»
8. ГОСТ 22505-83 «Радиопомехи индустриальные от приемников телевизионных и приемников радиовещательных частотно-модулированных сигналов в диапазоне УКВ. Нормы и методы измерений.»
9. Инструкция по эксплуатации измерителя шума и вибрации ВШВ-003-М3.
6. Инструкция по эксплуатации скоростного поискового приемника радиосигналов «Скорпион», БНТИ-ТСС, Москва, 2006.
10. Руководство пользователя комплекса «Омега», ОАО НОВО, Москва, 2005.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

3. http://www.biblioclub.ru
4. http://znanium.com
5. www.rucont.ru

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения*: MS Office.*

Информационные справочные системы:

1. Справочно-правовая система «Консультант плюс».
2. Электронные ресурсы образовательной среды Университета.