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 ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И УПРАВЛЯЮЩИХ СИСТЕМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.05.02 «КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ И ТЕХНОЛОГИЙ»

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: Логачева Н.В. Рабочая программа дисциплины (модуля): Компьютерное моделирование информационных процессов и технологий. – Королев МО: «Технологический Университет», 2023

Рецензент: Аббасова Т.С.

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)	Артюшенко В.М., д.т.н., проф.			
Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания кафедры	Протокол № 12 от 05.04.2023г.			

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:

овладение основными правилами, принципами, закономерностями, методами моделирования информационных процессов и технологий для обеспечения информационной безопасности;

умение эффективно использовать методы моделирования на практике.

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.

Основными задачами дисциплины являются:

- подготовить магистров к самостоятельному научному творчеству в области защищенности информационных систем;
- расширить представление в области организации научных исследований по моделированию информационных процессов и технологий;
- систематизировать знания в плане организации научных исследований и достижения результатов в процессе моделирования информационных систем и технологий;
- овладеть навыками решения творческих нетривиальных задач связанных с вопросами моделирования угроз информационным объектам и противодействия им .

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 проект-

ной 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, основной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационных технологий и управляющих систем.

Дисциплина базируется на ранее изученных дисциплинах «Основы теории информационной безопасности», «Специальные разделы математики», «Экспертные системы комплексной оценки безопасности автоматизированных и телекоммуникационных систем» и компетенциях: ПК-1, 3; УК-1, 2; ОПК-1.

Знания и компетенции, полученные при изучении дисциплины необходимы для написания магистерской диссертации.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины представлена в таблице 1 и составляет 2 зачетные 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.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1. Темы дисциплины и виды занятий

Темы дисциплины, количество часов на лекции и практические занятия приведены в таблице 2.

Таблица 2

Наименование тем	**Лекции, час.**	**Практ. занятия, час**	**Лаб. занятия час**	**Занятия в интерактивной форме**	**Практическая поготовка ,час**	**Код компетенций**
1	**2**	**3**	**4**	**5**	**6**	**7**
Тема 1. Модели информационных процессов. Определение и назначение компьютерного моделирования.	8	4	2	3	1	ПК-2
Тема 2. Этапы построения математической модели и решения задачи математического моделирования	4	4	4	3	1	ПК-2; ПК-3
Тема 3. Моделирование информационных процессов в условиях неопределенностей. Виды неопределенностей.	4	8	2	4	2	ПК-2; ПК-3
Итого:	**16**	**16**	8	10	4	

5.2. Содержание тем дисциплины

Тема 1. Определение и назначение моделирования.

Цель и задачи компьютерного моделирования информационных процессов. Определение моделей, их свойства и классификация. Математическое моделирование и его место в теории познания. Критерии оценок качества моделирования.

Тема 2. Этапы построения математической модели и решения задачи математического моделирования.

Обследование объекта моделирования. Математическая постановка задачи моделирования и построение модели информационного процесса. Выбор и обоснование метода решения задачи. Реализация математической модели в виде программы. Проверка адекватности построенной модели. Проведение моделирования информационных процессов и анализ его результатов. Примеры математических моделей и значимость результатов полученных с их помощью в результате математического моделирования.

Тема 3. Моделирование в условиях неопределенностей.

Причины неопределенностей и их виды. Моделирование в условиях стохастической неопределенности и неопределенностей описываемых с позиции теории чувствительности.

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

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

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

Структура фонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю) приведена в Приложении 1.

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

Основная литература:

1.Математическое моделирование технических систем: учебник / В.П. Тарасик. — Минск: Новое знание; М.: ИНФРА-М, 2018. — 592 с. — (Высшее образование: Бакалавриат) [электронный ресурс] // Режим доступа: http://znanium.com/catalog/product/952123

Дополнительная

2.Аверченков В.И. Основы математического моделирования технических систем / В.И. Аверченков, В.П. Федоров, М.Л. Хейфец. – 3-е изд., стер. – Москва: Издательство «Флинта», 2016. – 271 с.: схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93344

3. Голубева Н. В. Математическое моделирование систем и процессов: учебное пособие / Н. В. Голубева. — 2-е изд., стер. — Санкт-Петербург: Лань, 2016. — 192 с. — ISBN 978-5-8114-1424-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/76825

4. Чернышов В.Н. Моделирование информационных процессов и исследование в ИТ / В.Н. Чернышов, Д.В. Образцов, А.В. Платёнкин ; Министерство образования и науки Российской Феде-рации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». – Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2017. – 98 с.: ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=499294

Дополнительная литература:

5. Теоретические основы информационных процессов и систем / Душин В.К., - 5-е изд. - М.:Дашков и К, 2018. - 348 с.: ISBN 978-5-394-01748-3 - Режим доступа: http://znanium.com/catalog/product/450784

6.Моделирование систем и процессов: учебник для вузов/ В.Н. Волкова [и др.]; под редакцией В.Н. Волковой, В.Н. Козлова.— Москва: Издательство Юрайт, 2020 — 450с. — (Высшее образование). — ISBN 978-5-9916-7322-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450218

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

Интернет-ресурсы:

8.1. http:// www.akademy.it.ru/ – академия АЙТИ.

8.2. http://citforum.ru›nets/articles/cable.shtml Кабельные системы локальных вычислительных сетей

8.3. http:// www.cyberforum.ru Форум программистов и сисадминов

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

Рабочая программа и методическое обеспечение по дисциплине

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

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

Перечень программного обеспечения: *MSOffice, MatCad.*

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.

Прочее:

- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Практические занятия:

- Аудитория, оснащенная мультимедийными средствами (интерактивная доска).

- рабочее место преподавателя, оснащенное ПК с доступом в глобальную сеть Интернет;

- рабочие места студентов, оснащенные компьютерами с доступом в глобальную сеть Интернет и установленным программным обеспечением.

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 (модулю)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И УПРАВЛЯЮЩИХ СИСТЕМ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ
КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ И ТЕХНОЛОГИЙ

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	ПК-2	Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном исполнении	Тема 1-3	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-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности.	Тема:1,2,3	ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.	ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.	ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

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	Доклад в форме презентации	А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов Б) частично сформирована: • компетенция освоена на продвинутом уровне – 4 балла; • компетенция освоена на базовом уровне – 3 балла; В) не сформирована (компетенция не сформирована) – 2 и менее баллов	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 5- 10 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. Оценка проставляется в электронный журнал.
	Творческая работа	А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов Б) частично сформирована: • компетенция освоена на продвинутом уровне – 4 балла; • компетенция освоена на базовом уровне – 3 балла; В) не сформирована (компетенция не сформирована) – 2 и менее баллов	Проводится письменно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 90 мин. Неявка – 0. Критерии оценки: 1. Анализ и выводы, отражающие суть изучаемого явления с указанием конкретных результатов (1 балл). 2. Оформление работы в

			соответствии с требованиями и методическими указаниями (1 балл). 3. Качество выполненной работы (1 балл). 4. Умение применять выбранные методы (1 балл). 5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов – 5 баллов. Оценка проставляется в электронный журнал.
ПК-2; ПК-3	Лабораторная работа	А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов Б) частично сформирована: • компетенция освоена на продвинутом уровне – 4 балла; • компетенция освоена на базовом уровне – 3 балла; В) не сформирована (компетенция не сформирована) – 2 и менее баллов	Например: 1. Оформление в соответствии с требованиями (1 балл). 2. Выбор методов измерений и вычислений (1 балл). 3. Умение применять выбранные методы (1 балл). 4. Анализ и выводы, отражающие суть изучаемого явления с указанием конкретных результатов (2 балла). Максимальная оценка – 5 баллов.

ПК-2; ПК-3.	Решение задач	А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов Б) частично сформирована: • компетенция освоена на продвинутом уровне – 4 балла; • компетенция освоена на базовом уровне – 3 балла; В) не сформирована (компетенция не сформирована) – 2 и менее баллов	Занятие проводится с применением компьютерных технологий 1. Выбор оптимальных методов измерений переменных и анализа данных (1 балл). 2. Умение применять выбранные методы анализа данных (1 балл). 3. Логический ход решения задачи правильный, но имеются арифметические ошибки в расчетах (1 балл). 4. Анализ и выводы, отражающие суть изучаемого явления с указанием конкретных результатов (2 балл). 5. Задача не решена (0 баллов). 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 сов-

местно 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 про-

воднику 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.

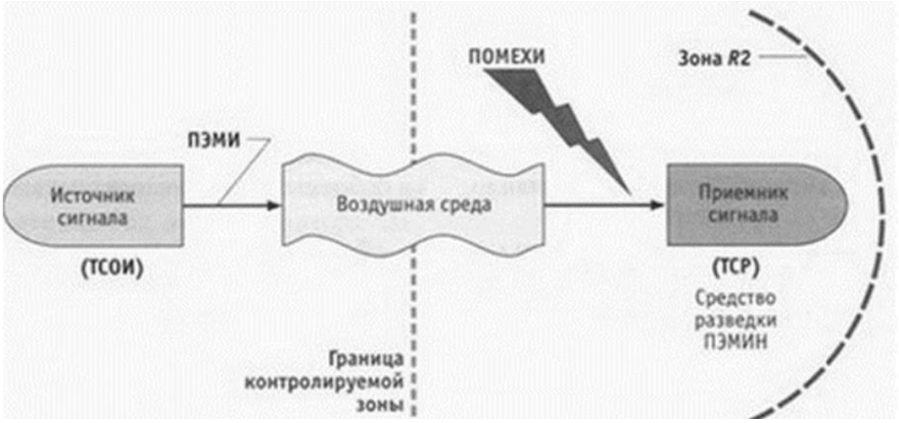

Рисунок 1. Схема ТКУИ за счет ПЭМИ

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

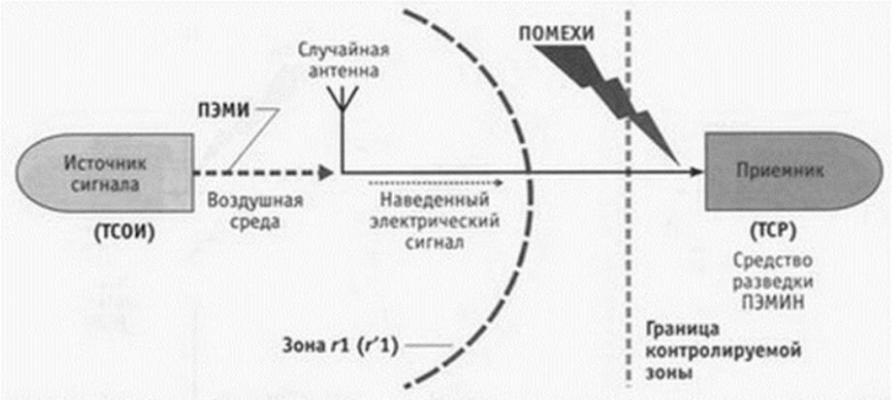

Рисунок 2. Схема ТКУИ за счет ПЭМИН

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»

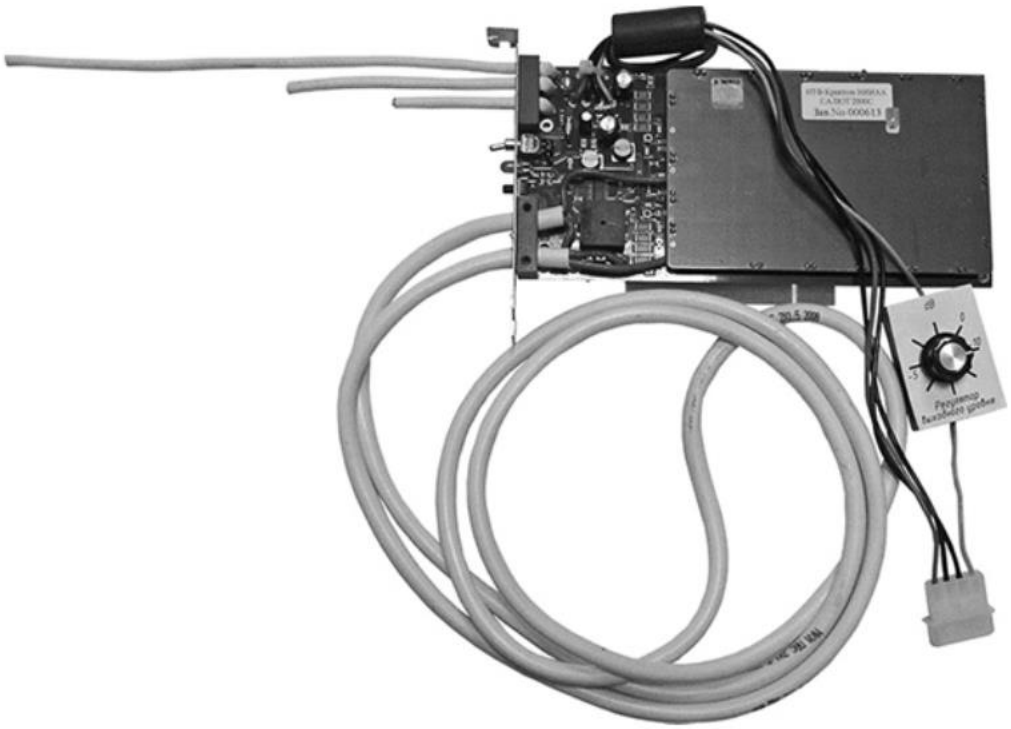

Рисунок 2. Средство активной защиты информации от утечек за счет ПЭМИН «Салют 2000С»

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?

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

Формой контроля знаний по дисциплине «Компьютерное моделирвание информационных процессов и технологий» являются две текущие аттестации в виде тестов и одна промежуточная аттестация в виде зачета в устной форме.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-2; ПК-3.	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – -30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-2; ПК-3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – -30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от***

						90%
Проводится в сроки, установленные графиком образовательного процесса	зачет	ПК-2; ПК-3	1 вопрос	Зачет проводится в устной форме. Время отведенное на процедуру – 30 минут на студента.	Результаты предоставляются в день проведения экзамена	Критерии оценки: 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; • 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.

Типовые вопросы, выносимые на зачет

1. Математическая постановка задачи моделирования.
2. Этапы обследования объекта при построении его математической модели.
3. Кибернитический подход к моделированию технологических процессов.
4. Какое моделирование называется математическим.
5. Чем отличается натурное моделирования от мысленного.
6. Почему информационные модели нельзя считать разновидностью математических моделей.
7. Чем простые математические модели отличаются от сложных.
8. Для каких целей используются оптимизационные модели.
9. Оптимизационная модель процесса и ее назначение.
10. Классификация математических моделей в зависимости от методов реализации.
11. Структурное моделирование.
12. Модель белого ящика и ее практическое использование
13. Что такое структурная схема и чем граф отличается от сети.
14. Модель черного ящика и ее практическое использование
15. Построить формальную модель педагогического процесса в вузе.
16. Операция декомпозиция и ее практическое использование при моделировании информационных процессов.
17. Временные структурные модели в экономике и промышленности.
18. Структурная схема системы.
19. Гармонический осциллятор- содержательная и математическая постановка задачи.
20. Модель конкуренции двух популяций.
21. Понятия устойчивости и неустойчивости стационарных состояний.
22. Понятие множественности стационарных состояний в процессах теплопередачи.
23. Модель Мальтуса и результаты ее анализа.
24. Модель спроса и предложения.
25. Статистический анализ простейших конструкций.
26. Причины возможной неадекватности математической модели.
27. Каким требованиям должна удолетворять корректная модель.
28. Выполните содержательную, концептуальную и математическую постановку задачи обеспечения информационной безопасности предприятия.
29. Проверка адекватности модели.
30. Этапы разработки программного обеспечения для анализа математичской модели
31. Язык формального описания алгоритмов.

Вариант 2.

1. Понятие модели и ее назначение.
2. Математическое моделирование, как инструмент познания мира.
3. Структурное моделирование.
4. Аналоговые модели.
5. Оптимизационные модели
6. Цифровое моделирование.
7. Этапы построения модели.
8. Алгоритмические модели.
9. Алгоритмы проверки адекватности моделей.
10. Кибернетический подход к моделированию технологических процессов.
11. Понятие системы.
12. Основные виды систем.
13. Устойчивость стационарных состояний
14. Множественность стационарных состояний объектов.
15. Язык формального описания алгоритмов.
16. Чувствительность стационарных состояний объектов.
17. Положительные обратные связи объекта моделирования.
18. Отрицательные обратные связи объекта моделирования.
19. Численные методы для анализа поведения математических моделей
20. Методы научного познания.
21. Свойства моделей.
22. Понятие адекватности математических моделей
23. Виды моделей.
24. Цели моделирования.
25. Классификация моделей.
26. Материальное моделирование.
27. Интуитивное моделирование
28. Идеальное моделирование.
29. Научное моделирование.
30. Знаковое моделирование.
31. Когнитные ,концептуальные и формальные модели.
32. Модель обеспечения информационной безопасности предприятия.
33. Логико-семантические модели.
34. Математическое моделирование.
35. Модель спроса и предложения.
36. Классификация математических моделей.
37. Параметры и переменные моделирования.
38. Понятие объекта моделирования как черный ящик.
39. Понятие объекта моделирования как белый ящик.

40. Сформулируйте содержательную постановку задачи работы ВУЗА.
41. Сформулируйте содержательную постановку задачи работы магазина.
42. Этапы построения математической модели.
43. Реализация математической модели в виде программы для ЭВМ.
44. МАТСАД-программный инструмент решения задач моделирования.
45. Чувствительность стационарных состояний.

Приложение 2
Методические указания для обучающихся по освоению дисциплины

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И УПРАВЛЯЮЩИХ СИСТЕМ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ И ТЕХНОЛИГИЙ

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 путем моделированния информационных процессов 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. План практических занятий

Практическое занятие 1.

Вид практического занятия**:** *подготовка доклада.*

Образовательные технологии: *практическая работа в группах*

Тема 1. Определение и назначение моделирования.

Цель занятия: компьютерное моделирование –инструмент определения возможных информационных угроз, их классификации и отработки технологии борьбы с ними.

Основные положения темы занятия: методы научного познания. Инструменты разработки модели-гипотеза, аналогия, понятия сходства и различия объектов, уровни абстрагирования Определение модели и моделирования.

Вопросы для обсуждения:

1.Моделирование-метод познания. Классификация моделей угроз и моделей-аналогов защиты реального объекта .

2. Аналогия-представление о сходстве объектов существенное или несущественное. Существенность сходства или различия сравниваемых объектов.

3.Защита информации с помощью шифрования. Шифрования файлов и папок. Антифишинг.

Продолжительность занятия – 5 ч.

Практическое занятие 2.

Вид практического занятия**:** *подготовка доклада.*

Образовательные технологии: *групповая дискуссия.*

Тема 2. Этапы построения математической модели и решения задачи математического моделирования.

Цель занятия: получение практических навыков при построении математических моделей информационных процессов.

Основные положения темы занятия:

1. Виды моделирования-материальное, аналоговое, интуитивное , научное.

2. Когнитные, концептуальные и формальные модели.

3. Классификации математических и информационных моделей.

4.Этапы построения модели.

Вопросы для обсуждения:

1.Обследование объекта моделирования.

2.Концептуальная постановка задачи моделироваия.

3.Математическая постановка задачи моделирования.

4. Выбор и обоснование выбора метода решения задачи моделирования.

5.Реализация модели в виде программы для ЭВМ.

6.Проверка адекватности математической модели.

7.Практическое использование математической модели и анализ результатов моделирования.

8. Примеры использования математических моделей информационных процессов.

Продолжительность занятия – 5 ч.

Практическое занятие 3.

Вид практического занятия**:** *подготовка доклада.*

Образовательные технологии: *беседа.*

Тема 3. Моделирование в условиях неопределенностей.

Цель занятия: решение типовых задач моделирования информационных процессов.

Основные положения темы занятия:

1.Причины появления неопределенностей и их виды.

2. Моделирование в условиях неопределенностей с позиции теории нечетких множеств.

Вопросы для обсуждения:

1. Решение типовой задачи.

Продолжительность занятия – 6 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 конфиденци-

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

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

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

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

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

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

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

– от несанкционированного доступа,

– от утечки по техническим каналам,

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

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

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

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

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

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

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

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

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

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

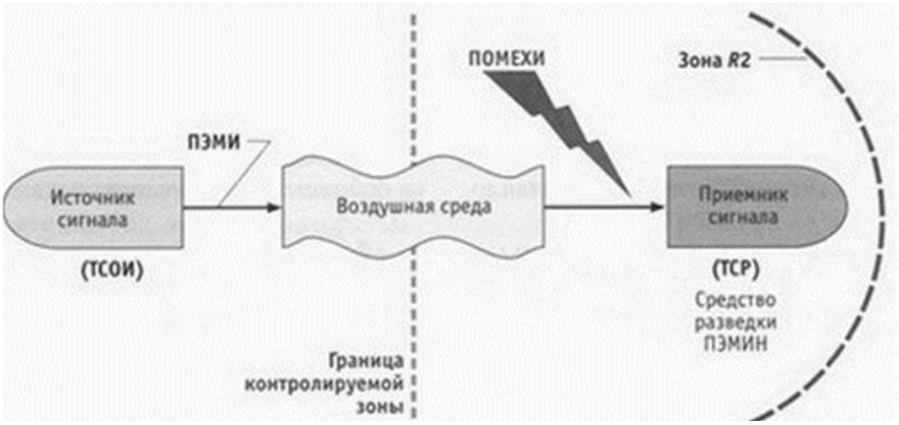

Рисунок 1. Схема ТКУИ за счет ПЭМИ

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

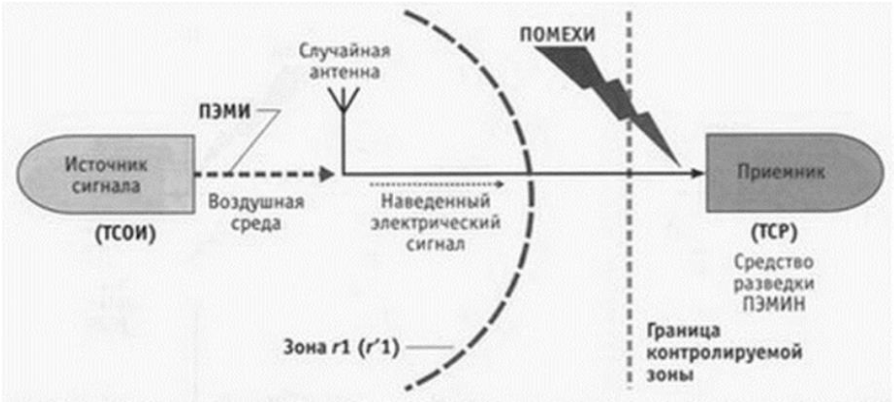

Рисунок 2. Схема ТКУИ за счет ПЭМИН

Поясним некоторые сокращения и термины на схемах:

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

• ТСР–технические средства разведки;

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

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

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

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

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

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

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

грифы СЕКРЕТНО и СОВЕРШЕННО СЕКРЕТНО. Вышеизложенный материал является открытым и считается опорным в общих знаниях ТЗИ.

Практическая часть.

Вопросы для самопроверки:

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	E-3000	30 МГц – 3000 МГц
Антенна электрическая дипольная	E-30	10 Гц – 30 МГц

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

Альтернативная измерительная площадка.

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

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

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

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

Измерительная площадка – площадка, отвечающая требованиям, обеспечивающим правильное измерение уровней индустриальных радиопомех (ИРП), излучаемых ТС в регламентированных условиях. Видов ИП предусматриваются два – «открытая измерительная площадка» и «альтернативная измерительная площадка». Поскольку строительство и эксплуатация открытой площадки весьма дорого, сосредоточимся на более дешёвом варианте –

АИП. Разница между открытой ИП и АИП заключается в том, что последняя должна размещаться не в открытом пространстве, а в некотором помещении, в здании. При том физические характеристики АИП (прежде всего «затухание» электромагнитного поля) должны оставаться в пределах установленного допуска.

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

Практическая часть.

Вопросы для самопроверки:

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
3 семестр		
1	Определение и назначение моделирования.	1. Оптимизационные модели 2. Цифровое моделирование. 3. Этапы построения модели. 4. Алгоритмические модели. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
2	Этапы построения математической модели и решения задачи математического моделирования.	1. Понятие системы. 2. Основные виды систем. 3. Устойчивость стационарных состояний *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
3	Моделирование в условиях неопределенностей	1. Свойства моделей. 2. Понятие адекватности математических моделей 3. Виды моделей. 4. Цели моделирования. 5. Классификация моделей. 6. Материальное моделирование. *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.Математическое моделирование технических систем: учебник / В.П. Тарасик. — Минск: Новое знание; М.: ИНФРА-М, 2018. — 592 с. — (Высшее образование: Бакалавриат) [электронный ресурс] // Режим доступа: http://znanium.com/catalog/product/952123

Дополнительная

2.Аверченков В.И. Основы математического моделирования технических систем / В.И. Аверченков, В.П. Федоров, М.Л. Хейфец. – 3-е изд., стер. – Москва: Издательство «Флинта», 2016. – 271 с.: схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93344

3. Голубева Н. В. Математическое моделирование систем и процессов: учебное пособие / Н. В. Голубева. — 2-е изд., стер. — Санкт-Петербург: Лань,

2016. — 192 с. — ISBN 978-5-8114-1424-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/76825
4. Чернышов В.Н. Моделирование информационных процессов и исследование в ИТ / В.Н. Чернышов, Д.В. Образцов, А.В. Платёнкин ; Министерство образования и науки Российской Феде-рации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». – Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2017. – 98 с.: ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=499294

Дополнительная литература:

5. Теоретические основы информационных процессов и систем / Душин В.К., - 5-е изд. - М.:Дашков и К, 2018. - 348 с.: ISBN 978-5-394-01748-3 - Режим доступа: http://znanium.com/catalog/product/450784
6.Моделирование систем и процессов: учебник для вузов/ В.Н. Волкова [и др.]; под редакцией В.Н. Волковой, В.Н. Козлова.— Москва: Издательство Юрайт, 2020 — 450с. — (Высшее образование). — ISBN 978-5-9916-7322-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450218

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

Интернет-ресурсы:

1. http://www. eup.ru–научно-образовательный портал.
2. http://www. informika.ru– образовательный портал.
3. Материалы сайта http://docs.moodle.org/overview
4. Материалы сайта studentsworks/
5. Материалы сайта cooldoclad.narod/

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

Перечень программного обеспечения*: MS Office.*

Информационные справочные системы:

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