Государственное бюджетное образовательное учреждение высшего образования Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

Подписано цифровой подписью: ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ "ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А.ЛЕОНОВА"

«УТВЕРЖДАЮ»
Проректор по учебно-методической работе
И.В. Бабина
_____ 2022 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.В.ДВ.09.01 «РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ И СРЕДСТВА КАК ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

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: Соляной В.Н. Рабочая программа дисциплины: «Радиоэлектронные системы и средства как объекты информационной безопасности». – Королев МО: «Технологический университет», 2022.

Рецензент: **Журавлев С.И.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 12.04.2022 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.т.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2022	2023	2024	2025
Номер и дата протокола заседания кафедры	№8 от 12.03.2022			

Рабочая программа согласована:

Руководитель ОПОП ВО к.т.н., доцент Вихров А.П.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2022	2023	2024	2025
Номер и дата протокола заседания УМС	№4 от 12.04.2022			

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

Целями изучения дисциплины является формирование у студентов базовых знаний и практических навыков в области радиотехнического контроля информационных систем.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

ПК-3. Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС;

ПК-5. Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений;

Основными **задачами** дисциплины являются:

1. Формирование у студентов базовых знаний в области радиотехнического контроля информационных систем;
2. Практическое ознакомление с современными техническими средствами радиотехнического контроля информационных систем.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;
- документационное обеспечение по разработке проектных решений по ЗИ, принципы и особенности организации проектно-технологической деятельности;

Необходимые умения:

- оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ;
- участвовать в разработке проектных документов на создание подсистемы ИБ с разработкой модели проектируемых систем ЗИ и осуществлять технико-экономическое обоснование;

Трудовые действия:

- анализировать воздействие на защищаемую систему информации, оценивать последствия и вырабатывать предложения по ее совершенствованию;
- анализировать защищенность информационной инфраструктуры с формированием системы требований по ЗИ и участвовать в обосновании критериев эффективности функционирования проектируемых систем ИБ

(ЗИ)

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Радиоэлектронные системы и средства как объекты информационной безопасности» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Электротехника», «Электроника и схемотехника», «Физика», «Математический анализ», «Теория вероятностей и математическая статистика», «Иностранный язык», «Нормативные акты и стандарты по информационной безопасности», и компетенциях: ОПК-2,3,4,8,11; УК-4; ДОПК-1,2,3,4.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность автоматизированных систем», «Моделирование процессов и систем защиты информации», «Нормативные акты и стандарты по информационной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 3 зачетных единиц 108 часов.

Таблица1

Виды занятий	Всего часов	Семестр 5	Семестр …	Семестр 9	Семестр …
Общая трудоемкость	108	108		108	
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48	48			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	32	32			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	50	50			
Другие виды контактной работы	**10**	**10**			
Практическая подготовка	-	-			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+ -	+ -			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	Т1; Т2	Т1; Т2			
Вид итогового контроля	Зачет	Зачет			

4. Содержание дисциплины
4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. очное	Практические занятия, час. очное	Занятия в интерактивной форме, час. очное	Код компетенций
1	2	3	4	5
Раздел 1. Основы технического контроля функционирования радиоэлектронных систем и средств				
Тема 1. Сущность и содержание радиотехнического контроля	4	8	2	ПК-3
Тема 2. Нормативно - правовое обеспечение радиотехнического контроля функционирования информационных систем (объектов)	4	8	2	ПК-3
Раздел 2. Организация и технологии радиоэлектронной защиты современных информационных систем.				
Тема 3. Основы организации радиотехнического контроля функционирования информационных систем	4	8	4	ПК-5
Тема 4. Базовые технологии обеспечения радиоэлектронной безопасности функционирования информационных систем	4	8	2	ПК-5
	16	32	10	

4.2. Содержание тем дисциплины
<u>Раздел 1.</u> Основы технического контроля функционирования радиоэлектронных систем и средств

Тема 1. Сущность и содержание радиотехнического контроля

Назначение и содержание технического контроля. Основные положения и направления технического контроля эффективности принимаемых мер по безопасности функционирования РЭС на информационных объектах.

Тема 2. Нормативно - правовое обеспечение радиотехнического контроля функционирования информационных систем (объектов)

Состав и требования ведомственных нормативных документов по техническому контролю функционирования радиоэлектронных систем и

средств на информационных объектах.

Общая характеристика отрабатываемых документов по радиоэлектронной защите информационных систем (объектов).

Раздел 2. Организация и технологии радиоэлектронной защиты современных информационных систем.

Тема 3. Основы организации радиотехнического контроля функционирования информационных систем

Организация технического контроля по защите от радиотехнической, радио, радиолокационной и инфракрасной разведок.

Оценка обстановки и обоснование целесообразных мер по радиоэлектронной защите.

Планирование мероприятий по радиоэлектронной безопасности и, контроль за реализацией принятых мер по радиоэлектронной защите.

Оценка эффективности проводимых мер по обеспечению радиоэлектронной безопасности функционирования информационных объектов.

Тема 4. Базовые технологии обеспечения радиоэлектронной безопасности функционирования информационных систем

Привлекаемые силы и средства по обеспечению радиоэлектронной защиты.

Радиомониторинг функционирования информационных объектов (задачи, методы и средства).

Основы оценки эффективности вскрытия функционирования РЭС информационных систем различными видами радиоэлектронной разведки

Основные положения по обеспечению электромагнитной совместимости (ЭМС) функционирования радиоэлектронных средств в информационных системах. Непреднамеренные электромагнитные межсистемные помехи: источники и рецепторы.

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 «Радиоэлектронные системы и средства как объекты информационной безопасности», приведена в Приложении 1.

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

Основная литература:

1. Казаринова Ю.Н. Радиотехнические системы: учебник под ред. Ю.Н. Казаринова. – М.: Издательский центр «Академия», 2008.
2. Малюк А.А., Горбатов В.С. Введение в информационную безопасность : Учебное пособие для вузов / Под ред. В. С. Горбатова. - М. : Горячая линия - Телеком, 2013.
3. Васильев Р. Б., Калянов Г. Н., Стратегическое управление информационными системами: Учебник / -М : ИНТУИТ, 2014.

Дополнительная литература:

1. Куприянов А. И., Шевцов В. А., Сахаров А. В. Основы защиты информации. / – М.: Академия, 2010.
2. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации: Учебное пособие. М.: «Академия», 2007.

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

Интернет-ресурсы:

1. www.fstec.ru – Официальный сайт ФСТЭК России.
2. www.securityforum.org - (лучшие практики, исследования, отчеты, методологии).

9. Методические указания для обучающихся по освоению дисциплины

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. Ресурсы информационно-образовательной среды МГОТУ
2. Рабочая программа и методическое обеспечение по курсу: «Радиоэлектронные системы и средства как объекты информационной безопасности»
3. Учебный портал с электронно-методическими комплексами (do.kimes).
4. Универсальная библиотека онлайн (www.biblioclub.ru).
5. Polpred.com www.polpred.com.

6. Единое окно доступа (www.window.edu.ru)/
7. Издательский дом «Гребенников» (http://grebennikon.ru/)..

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

Приложение 1

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

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ И СРЕДСТВА КАК ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

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-3	Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС	Темы 1,2,3,4	- анализировать воздействие на защищаемую систему информации, оценивать последствия и вырабатывать предложения по ее совершенствованию	- оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ;	- основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;
2.	ПК-5	Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении обоснования соответствующих проектных решений	Темы 1,2,3, 4	- Анализировать защищенность информационной инфраструктуры с формированием системы требований по ЗИ и участвовать в обосновании критериев эффективности функционирования проектируемых систем ИБ (ЗИ)	- Участвовать в разработке проектных документов на создание подсистемы ИБ с разработкой модели проектируемых систем ЗИ и осуществлять технико-экономическое обоснование;	- Документационное обеспечение по разработке проектных решений по ЗИ, принципы и особенности организации проектно-технологической деятельности;

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

Код компетенции	*Инструмент, оценивающий сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
ПК-3,5	***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-3,5	***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***	***Например:*** ***Проводится в письменной и/или устной форме.*** ***Критерии оценки:*** ***1. Соответствие содержания доклада заявленной тематике (1 балл).*** ***2. Качество источников и их количество при подготовке работы (1 балл).*** ***3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).*** ***4. Качество самой представленной работы (1 балл).*** ***5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).***

			Максимальная сумма баллов - 5 баллов.
ПК-3,5	***Выполнение контрольной работы***	***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***	***При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида***

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 презентационной форме:

1. современные комплексы контроля защищенности радиотехнических систем;
2. безопасность автоматизированных радиотехнических систем;
3. программно-аппаратные методы защиты радиотехнических систем;
4. математическое моделирование радиотехнических систем;
5. технические средства контроля радиотехнических систем;
6. принципы работы радиотехнических систем;
7. современные проблемы обеспечения безопасности радиотехнических систем;

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

Формой контроля знаний по дисциплине «Радиоэлектронные системы и средства как объекты информационной безопасности» 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
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-3,5	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-3,5	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 образо	Зачет	ПК-3,5	20 вопросов	Компьютерное тестирование; время отведенное на процедуру –	Результаты тестирования предоставляются в день проведения	Критерии оценки: **«Зачтено»:** 1. знание лексического и грамматического материала; 2. умение использовать и применять

ватель ного процес са				30 минут	процедуры	полученные знания на практике; 3. работа на практических занятиях в течение семестра; 4. ответ на вопросы зачета. **«Не зачтено»:** 1. демонстрирует частичные знания по темам дисциплин; 2. незнание лексического и грамматического материала; 3. неумение использовать и применять полученные знания; 4. не работал на практических занятиях; 5. не отвечает на вопросы зачета.

Примерное содержание тестов для текущей аттестации:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

1. Что следует понимать под системой защиты информации?
2. Что понимают под радиоэлектронной безопасностью?
2. Что понимают под дезинформацией?
3. Что понимают под радиоэлектронной защитой?
4. Как изменяется ценность информации во времени?
5. Сущность радиотехнического контроля информационной системы?
6. Что называется тезаурусом?
7. Сущность радиотехнического контроля информационного объекта?
8. Определение радиоэлектронного противодействия?
9. Что называют утечкой информации?
10. Основные принципы радиоэлектронной безопасности?
11. Основные задачи радиоэлектронной безопасности?
12. Что называют перехватом?
13. Основные функции радиоэлектронной безопасности?
14. Что понимают под основными техническими средствами и системами?
15. Субъекты радиоэлектронной безопасности?
16. Что называют каналом утечки информации?
17. Оценка радиоэлектронной безопасности?
18. Укажите правильный перечень технических каналов утечки

информации?

19. Основные мероприятия по обеспечению радиоэлектронной безопасности?

20. Какой из показателей не является показателем технического канала утечки информации?

Типовые вопросы, выносимые на зачет.

1. Характеристики технических средств, влияющие на эффективность добывания информации.
2. Сущность и содержание радиотехнического контроля
3. Классификация средств добывания информации.
4. Основы технического контроля функционирования радиоэлектронных систем и средств
5. Технические характеристики средств добывания информации.
6. Назначение и содержание технического контроля.
7. Структура системы технической разведки. Основные функции органов планирования и управления, сбора, добывания и обработки информации.
8. Основные положения и направления технического контроля эффективности принимаемых мер по безопасности функционирования РЭС на информационных объектах.
9. Принципы радиолокационного наблюдения.
10. Нормативно - правовое обеспечение радиотехнического контроля функционирования информационных систем (объектов)
11. Радиотеплолокационное наблюдение.
12. Оценка радиоэлектронной безопасности?
13. Состав и требования ведомственных нормативных документов по техническому контролю функционирования радиоэлектронных систем и средств на информационных объектах.
14. Структура системы средств перехвата радиосигналов, состав ее элементов.
15. Общая характеристика отрабатываемых документов по радиоэлектронной защите информационных систем (объектов).
16. Радиоприемные устройства и их характеристики.
17. Средства обнаружения излучений закладных устройств.
18. Структурная схема прибора радиационной разведки.
19. Организация инженерно-технической защиты информации на предприятиях. Типовая структура службы безопасности предприятия и основные функции ее подразделений.
20. Средства противодействия радиолокационному наблюдению.
21. Характеристики технических средств, влияющие на эффективность добывания информации.
22. Сущность и содержание радиотехнического контроля
23. Классификация средств добывания информации.
24. Основы технического контроля функционирования радиоэлектронных систем и средств

25. Технические характеристики средств добывания информации.
26. Назначение и содержание технического контроля.
27. Структура системы технической разведки. Основные функции органов планирования и управления, сбора, добывания и обработки информации.
28. Основные положения и направления технического контроля эффективности принимаемых мер по безопасности функционирования РЭС на информационных объектах.
29. Принципы радиолокационного наблюдения.
30. Нормативно - правовое обеспечение радиотехнического контроля функционирования информационных систем (объектов)
31. Радиотеплолокационное наблюдение.
32. Состав и требования ведомственных нормативных документов по техническому контролю функционирования радиоэлектронных систем и средств на информационных объектах.
33. Структура системы средств перехвата радиосигналов, состав ее элементов.
34. Общая характеристика отрабатываемых документов по радиоэлектронной защите информационных систем (объектов).
35. Радиоприемные устройства и их характеристики.
36. Организация и технологии по радиоэлектронной защиты современных информационных систем.
37. Структурная схема прибора радиационной разведки.
38. Основы организации радиотехнического контроля функционирования информационных систем
39. Средства противодействия радиолокационному наблюдению.
40. Организация технического контроля по защите от радиотехнической разведки
41. Организация технического контроля по защите от радиолокационной разведки
42. Организация технического контроля по защите от радио разведки
43. Организация технического контроля по защите от инфракрасной разведки
44. Оценка обстановки и обоснование целесообразных мер по радиоэлектронной защите.
45. Средства обнаружения излучений закладных устройств.
46. Планирование мероприятий по радиоэлектронной безопасности
47. Организация инженерно-технической защиты информации на предприятиях. Типовая структура службы безопасности предприятия и основные функции ее подразделений.
48. Контроль за реализацией принятых мер по радиоэлектронной защите.
49. Оценка эффективности проводимых мер по обеспечению радиоэлектронной безопасности функционирования информационных объектов.

50. Базовые технологии обеспечения радиоэлектронной безопасности функционирования информационных систем

51. Привлекаемые силы и средства по обеспечению радиоэлектронной защиты.

52. Задачи радио мониторинга функционирования информационных объектов

53. Методы радио мониторинга функционирования информационных объектов

54. Средства радио мониторинга функционирования информационных объектов

55. Основы оценки эффективности вскрытия функционирования РЭС информационных систем различными видами радиоэлектронной разведки

56. Основные положения по обеспечению электромагнитной совместимости (ЭМС) функционирования радиоэлектронных средств в информационных системах

57. Источники непреднамеренных электромагнитных межсистемных помех

58. Рецепторы непреднамеренных электромагнитных межсистемных помех

**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.*

Приложение 2

Методические указания для обучающихся по освоению дисциплины (модуля)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ И СРЕДСТВА КАК ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Безопасность телекоммуникационных систем (в аэрокосмической сфере)
Уровень высшего образования: бакалавр
Форма обучения: очная

Королев
2022

1. Общие положения

Целями изучения дисциплины является:

– формирование у студентов базовых знаний и практических навыков в области радиотехнического контроля информационных систем.

– ознакомление студентов с современными средствами защиты информации и радиотехнического контроля информационных систем.

Задачами дисциплины являются:

1. Формирование у студентов базовых знаний в области радиотехнического контроля информационных систем.
2. Практическое ознакомление с современными техническими средствами радиотехнического контроля информационных систем.

2. Указания по проведению практических занятий

Практическое занятие 1.

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

Образовательные технологии: ***групповая дискуссия.***

Тема: Сущность и содержание радиотехнического контроля

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

Тема и содержание практического занятия:

Цель работы: Получить практические умения выбора методов и средств радиотехнического контроля информационных систем.

Основные положения темы занятия:

1. методы радиотехнического контроля информационных систем.
2. средства реализации методов радиотехнического контроля информационных систем.

Вопросы для обсуждения:

1. назначение технического контроля
2. содержание технического контроля
3. основные положения технического контроля
4. основные направления технического контроля
5. контроль эффективности принимаемых мер по безопасности
6. контроль безопасности функционирования РЭС
7. принципы построения системы обеспечения безопасности в информационной системе;
8. достоинства и недостатки различных видов мер защиты

Продолжительность занятия: 4 ч.

Практическое занятие 2.

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

Образовательные технологии: ***групповая дискуссия.***

Тема: Нормативно - правовое обеспечение радиотехнического контроля

функционирования информационных систем (объектов)

.

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки поиска, анализа и применения нормативно - правового обеспечение радиотехнического контроля.

Основные положения темы занятия:

1. Состав ведомственных нормативных документов по техническому контролю функционирования радиоэлектронных систем
2. Требования ведомственных нормативных документов по техническому контролю функционирования радиоэлектронных систем

Вопросы для обсуждения:

i. нормативные акты в области обеспечения радиотехнического контроля
ii. состав и содержание документов технического контроля
iii. правовые акты в области обеспечения радиотехнического контроля
iv. законодательные акты обеспечения радиотехнического контроля
v. обзор существующих правовых документов обеспечения радиотехнического контроля
vi. обзор постановлений правительства, законов и других руководящих документов.
vii. общая характеристика отрабатываемых документов по радиоэлектронной защите информационных систем

Продолжительность занятия: 4 ч.

Практическое занятие 3

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

Образовательные технологии: ***групповая дискуссия.***

Тема: Основы организации радиотехнического контроля функционирования информационных систем

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки организации радиотехнического контроля.

Основные положения темы занятия:

1. Организация контроля функционирования защиты от средств технических разведок.
2. обоснование целесообразных мер по радиоэлектронной защите.

Вопросы для обсуждения:

1. организация технического контроля по защите от радиотехнической, разведки
2. организация технического контроля по защите от радио разведки
3. организация технического контроля по защите от радиолокационной разведки

4. организация технического контроля по защите от инфракрасной разведки
5. оценка обстановки радиоэлектронной защиты
6. планирование мероприятий по радиоэлектронной безопасности
7. контроль за реализацией принятых мер по радиоэлектронной защите
8. оценка эффективности проводимых мер по обеспечению радиоэлектронной безопасности

Продолжительность занятия: 4 ч.

Практическое занятие 4

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

Образовательные технологии: ***групповая дискуссия.***

Тема: Базовые технологии обеспечения радиоэлектронной безопасности функционирования информационных систем

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки выбора и реализации технологий обеспечения радиоэлектронной безопасности.

Основные положения темы занятия:

1. Привлекаемые силы по обеспечению радиоэлектронной защиты.
2. Привлекаемые средства по обеспечению радиоэлектронной защиты.

Вопросы для обсуждения:

1. задачи радиомониторинга функционирования информационных объектов
2. методы радиомониторинга функционирования информационных объектов
3. средства радиомониторинга функционирования информационных объектов
4. Основы оценки эффективности вскрытия функционирования РЭС
5. Основные положения по обеспечению электромагнитной совместимости
6. источники непреднамеренных электромагнитных межсистемных помех
7. рецепторы непреднамеренных электромагнитных межсистемных помех.

Продолжительность занятия: 4 ч.

3. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	**Тема 1. Сущность и содержание радиотехнического контроля**	***Подготовка докладов по темам:*** 1. современные комплексы контроля защищенности информационных объектов по радио каналу; 2. современные комплексы контроля защищенности информационных объектов по радиотехническому каналу;

		3. современные комплексы контроля защищенности информационных объектов по радиоэлектронному каналу. 4. современные комплексы контроля защищенности информационных объектов по инфракрасному каналу.
2.	**Тема 2. Нормативно - правовое обеспечение радиотехнического контроля функционирования информационных систем (объектов)**	***Подготовка докладов по темам:*** 1. методы и средства радионаблюдения; 2. типовая структура радиотехнического канала утечки информации; 3. основные показатели радиотехнических каналов утечки информации; 4. простые и составные каналы утечки информации; 5. радиоэлектронный канал утечки информации;
3	**Тема 3. Основы организации радиотехнического контроля функционирования информационных систем**	***Подготовка докладов по темам:*** 1. материально-вещественный канал утечки информации; 2. методы и средства защиты информации от подслушивания; 3. методы и средства защиты информации от наблюдения; 4. методы и средства защиты информации от перехвата; 5. методы и средства контроля защищенности информации от утечки по техническим каналам.
4	**Тема 4. Базовые технологии обеспечения радиоэлектронной безопасности функционирования информационных систем**	***Подготовка докладов по темам:*** 1. Методы поиска и локализации излучающих закладных радиоустройств. 2. Методы поиска и локализации неизлучающих закладных радиоустройств. 3. Средства поиска и локализации излучающих закладных радиоустройств. 4. Средства поиска и локализации неизлучающих закладных радиоустройств. 5. Методика проведения специальных исследований защищенности информационного объекта от утечки по радиотехническому каналу. 6. Методика проведения специальных исследований защищенности информационного объекта от утечки по инфракрасному каналу.

		7. Методика проведения специальных исследований защищенности информационного объекта от утечки по радио каналу. 8. Методика проведения специальных исследований защищенности информационного объекта от утечки по радиоэлектронному каналу.

4. Указания по проведению контрольных работ

4.1. Требование к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

4.2. 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, сформированных 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 и оформлен с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

4.3. Требования к оформлению

Объем контрольной работы – 10-15 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

4.4.Примерная тематика контрольных работ:

1. Характеристики технических средств, влияющие на эффективность добывания информации.

2. Сущность и содержание радиотехнического контроля
3. Классификация средств добывания информации.
4. Основы технического контроля функционирования радиоэлектронных систем и средств
5. Технические характеристики средств добывания информации.
6. Назначение и содержание технического контроля.
7. Структура системы технической разведки. Основные функции органов планирования и управления, сбора, добывания и обработки информации.
8. Основные положения и направления технического контроля эффективности принимаемых мер по безопасности функционирования РЭС на информационных объектах.
9. Принципы радиолокационного наблюдения.
10. Нормативно - правовое обеспечение радиотехнического контроля функционирования информационных систем (объектов)
11. Радиотеплолокационное наблюдение.
12. Оценка радиоэлектронной безопасности?
13. Состав и требования ведомственных нормативных документов по техническому контролю функционирования радиоэлектронных систем и средств на информационных объектах.
14. Структура системы средств перехвата радиосигналов, состав ее элементов.
15. Общая характеристика отрабатываемых документов по радиоэлектронной защите информационных систем (объектов).
16. Радиоприемные устройства и их характеристики.
17. Средства обнаружения излучений закладных устройств.
18. Структурная схема прибора радиационной разведки.
19. Организация инженерно-технической защиты информации на предприятиях. Типовая структура службы безопасности предприятия и основные функции ее подразделений.
20. Средства противодействия радиолокационному наблюдению.
21. Характеристики технических средств, влияющие на эффективность добывания информации.
22. Сущность и содержание радиотехнического контроля
23. Классификация средств добывания информации.
24. Основы технического контроля функционирования радиоэлектронных систем и средств
25. Технические характеристики средств добывания информации.
26. Назначение и содержание технического контроля.
27. Структура системы технической разведки. Основные функции органов планирования и управления, сбора, добывания и обработки информации.
28. Основные положения и направления технического контроля эффективности принимаемых мер по безопасности функционирования РЭС на информационных объектах.

29. Принципы радиолокационного наблюдения.

30. Нормативно - правовое обеспечение радиотехнического контроля функционирования информационных систем (объектов)

31. Радиотеплолокационное наблюдение.

32. Состав и требования ведомственных нормативных документов по техническому контролю функционирования радиоэлектронных систем и средств на информационных объектах.

33. Структура системы средств перехвата радиосигналов, состав ее элементов.

34. Общая характеристика отрабатываемых документов по радиоэлектронной защите информационных систем (объектов).

35. Радиоприемные устройства и их характеристики.

36. Организация и технологии по радиоэлектронной защиты современных информационных систем.

37. Структурная схема прибора радиационной разведки.

38. Основы организации радиотехнического контроля функционирования информационных систем

39. Средства противодействия радиолокационному наблюдению.

40. Организация технического контроля по защите от радиотехнической разведки

41. Организация технического контроля по защите от радиолокационной разведки

42. Организация технического контроля по защите от радио разведки

43. Организация технического контроля по защите от инфракрасной разведки

44. Оценка обстановки и обоснование целесообразных мер по радиоэлектронной защите.

45. Средства обнаружения излучений закладных устройств.

46. Планирование мероприятий по радиоэлектронной безопасности

47. Организация инженерно-технической защиты информации на предприятиях. Типовая структура службы безопасности предприятия и основные функции ее подразделений.

48. Контроль за реализацией принятых мер по радиоэлектронной защите.

59. Оценка эффективности проводимых мер по обеспечению радиоэлектронной безопасности функционирования информационных объектов.

60. Базовые технологии обеспечения радиоэлектронной безопасности функционирования информационных систем

61. Привлекаемые силы и средства по обеспечению радиоэлектронной защиты.

62. Задачи радио мониторинга функционирования информационных объектов

63. Методы радио мониторинга функционирования информационных объектов

64. Средства радио мониторинга функционирования информационных объектов

65. Основы оценки эффективности вскрытия функционирования РЭС информационных систем различными видами радиоэлектронной разведки

66. Основные положения по обеспечению электромагнитной совместимости (ЭМС) функционирования радиоэлектронных средств в информационных системах

67. Источники непреднамеренных электромагнитных межсистемных помех

68. Рецепторы непреднамеренных электромагнитных межсистемных помех

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

Основная литература:

1. Казаринова Ю.Н. Радиотехнические системы: учебник под ред. Ю.Н. Казаринова. – М.: Издательский центр «Академия», 2008.

2. Малюк А.А., Горбатов В.С. Введение в информационную безопасность : Учебное пособие для вузов / Под ред. В. С. Горбатова. - М. : Горячая линия - Телеком, 2013.

3. Васильев Р. Б., Калянов Г. Н., Стратегическое управление информационными системами: Учебник / -М : ИНТУИТ, 2014.

Дополнительная литература:

1. Куприянов А. И., Шевцов В. А., Сахаров А. В. Основы защиты информации. / – М.: Академия, 2010.

2. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации: Учебное пособие. М.: «Академия», 2007.

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

Интернет-ресурсы:

- www.fstec.ru – Официальный сайт ФСТЭК России.
- www.securityforum.org - (лучшие практики, исследования, отчеты, методологии).

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

Перечень программного обеспечения: *MSOffice, PowerPoint.*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды Университета.
2. Рабочая программа и методическое обеспечение по дисциплине «Радиоэлектронные системы и средства как объекты информационной безопасности».
3. Учебный портал с электронно-методическими комплексами (do.kimes).
4. Универсальная библиотека онлайн (www.biblioclub.ru).
5. Polpred.com www.polpred.com.
6. Единое окно доступа (www.window.edu.ru)/
7. Издательский дом «Гребенников» (http://grebennikon.ru/)..