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

Троицкий Александр Витальевич

Подписано цифровой подписью: Троицкий Александр Витальевич

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

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ (МОДУЛЯ)

ФТД.В.01 «ОСНОВЫ РЭБ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль): Менеджмент информационной безопасности

Уровень высшего образования: Магистратура

Форма обучения: очная

Королев
2023

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

Автор: Соляной В.Н. Рабочая программа дисциплины: Основы РЭБ в информационной безопасности. – Королев МО: «Технологический Университет», 2023

Рецензент: к.в.н., доцент Воронов А.Н.

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

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Соляной В.Н. к.в.н. доцент			
Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания кафедры	№8 от 30.03.2023г.			

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

Рабочая программа рекомендована на заседании УМС:

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

2

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

Целью изучения дисциплины является углубленное изучение теоретических и прикладных основ социальной инженерии как научной дисциплины, связанной с созданием средств и методов выработки научно обоснованных управленческих решений в области информационной безопасности

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

Профессиональные компетенции:

- ПК-1: Способен организовывать выполнение работ, управлять коллективом 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:

- формирование у студентов базовых знаний в области радиотехнического контроля информационных систем;
- практическое ознакомление с современными техническими средствами радиотехнического контроля информационных систем.

Показатель освоения компетенции отражают следующие индикаторы:
Трудовые действия:

- ПК-1.3. Управлять работой коллектива профессионалов ИБ, разрабатывать нормативно-методические документы по функционированию автоматизированной ИАС, формировать комплекс мер по информационной защите автоматизированной ИАС с разработкой частных политик безопасности компьютерных систем

- ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.

Необходимые умения:

- ПК-1.2. Работать в коллективе, разрабатывать организационно-управленческие документы, принимать управленческие решения, реализовывать целесообразные меры противодействия информационным угрозам с применением национальных и международных стандартов в области ЗИ, оценивать их эффективность.

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

Необходимые знания:

- ПК-1.1. Знать научные основы, методы и технологии управленческой деятельности, нормативную базу по созданию и эксплуатацию защищенных автоматизированных ИАС, принципы и методы организации работ по ЗИ в ИАС, основные средства и способы организационного обеспечения ИБ, источники и классификацию угроз ИБ.

.- 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 в структуре ОПОП ВО

Дисциплина относится к факультативам основной профессиональной образовательной программы подготовки магистров по направлению подготовки «Информационная безопасность».

Дисциплина базируется на ранее изученных дисциплинах «Специальные разделы физики», «Специальные разделы математики», «Защищенные информационные системы», «Основы теории информационной безопасности» и компетенциях: УК-1; УК-2; УК-4; ОПК-1; ОПК-2 и ПК-1; ПК-3.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при дальнейшем изучении дисциплин общенаучного цикла «Комплексная проверка информационной безопасности», «Концептуальное проектирование технологий обеспечения информационной безопасности», и для написания магистерской диссертации.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа

Таблица 1

Виды занятий	Всего часов	Семестр 2	Семестр …	Семестр …	Семестр …
Общая трудоемкость	**72**	**72**			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**40**	**40**			
Лекции (Л)	**16**	**16**			
Практические занятия (ПЗ)	**24**	**24**			
Лабораторные работы (ЛР)	**нет**	**нет**			
Другие виды контактной работы*	**6**	**6**			
Практическая подготовка	**4**	**4**			
Самостоятельная работа	**32**	**32**			
***Курсовые работы (проекты)* ***					
Расчетно-графические работы*					
***Контрольная работа** *					
***Текущий контроль знаний** *	**Тест**	**Тест**			
Вид итогового контроля	**Зачет**	**Зачет**			

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

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. очное	Практические занятия, час. очное	Занятия в интерактивной форме, час. очное	Практическая поготовка ,час	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	6	1	1	ПК-1
Тема 2. Нормативно - правовое обеспечение радиотехнического контроля функционирования информационных систем (объектов)	**4**	6	1	1	ПК-1.
Раздел 2. Организация и технологии радиоэлектронной защиты современных информационных систем.					
Тема 3. Основы организации радиотехнического контроля функционирования информационных систем	4	6	2	1	ПК-3.
Тема 4. Базовые технологии обеспечения радиоэлектронной безопасности функционирования информационных систем	4	3	2	1	ПК-1,3
	16	24	6	**4**	

4.2. Содержание тем дисциплины

Раздел 1. 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 (модулю)

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» 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 «Основы РЭБ в информационной безопасности», приведена в Приложении 1.

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

Основная литература:

1.Овсянников, С. В.Проектирование систем наведения радиотехнических и оптических комплексов. Ч. 2 : учеб. пособие по курсу «Проектирование мехатронных систем» / Овсянников С. В. - М. : Изд-во МГТУ им. Н.Э. Баумана, 2009. - 48 : нет. - ISBN ----. - Электронная программа (визуальная). Электронные данные : электронные.
URL: https://lib.rucont.ru/efd/287519

2.Стасенко, И. В.Радиоэлектронные системы и устройства / Стасенко И. В. - М. : Изд-во МГТУ им. Н.Э. Баумана, 2013. - 44 : нет. - ISBN 978-5-7038-3685-9. - Электронная программа (визуальная). Электронные данные : электронные. URL: https://lib.rucont.ru/efd/287592
3.Статистический анализ и синтез радиотехнических устройств и систем: учебное пособие для вузов / В. И. Тихонов, В.Н. Харисов. — М.: Горячая линия-Телеком, 2014. — 608 с.

Дополнительная литература:

4.Электродинамика и распространение радиоволн : учебное пособие / Д.Ю. Муромцев, Ю.Т. Зырянов, П.А. Федюнин и др. – Тамбов : Изд-во ФГБОУ ВПО «ТГТУ», 2012. – 200 с
5.Теория оптимальных методов радиоприема при флуктуационных помехах / Л.С. Гуткин. — М.: Сов. радио, 1972. — 447 с.
Теоретические основы радиолокации и радионавигации: Учеб. пособие для радиотехн. спец. вузов / Ю. Г. Сосулин. — М.: Радио и связь, 1992. — 303 с.

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

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 (модуля)

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

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

Перечень программного обеспечения: *MSOffice, PowerPoint.*

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета
2. Рабочая программа и методическое обеспечение по дисциплине: «Основы РЭБ в 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.

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 ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

ОСНОВЫ РЭБ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль: Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев

2023

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

№ п/п	Индекс компетенции	Содержание компетенции*	Раздел дисциплины, обеспечивающий формирование компетенции)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ПК-1	Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении.	Темы 1-4	ПК-1.3. Управлять работой коллектива профессионало в ИБ, разрабатывать нормативно-методические документы по функционированию автоматизированной ИАС, формировать комплекс мер по информационной защите автоматизированной ИАС с разработкой частных политик безопасности компьютерных систем.	ПК-1.2. Работать в коллективе, разрабатывать организационно-управленческие документы, принимать управленческие решения, реализовывать целесообразные меры противодействия информационным угрозам с применением национальных и международных стандартов в области ЗИ, оценивать их эффективность.	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.	ПК-3	Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в	Тема 1- 4	ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка	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-

		области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности.		труда.		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-1,3	Доклад в форме презентации	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.

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 «Основы радиоэлектронной борьбы в 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
Согласно учебному плану	тестирование	ПК-1 ПК-3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным***

						соотношением. ***Неявка – 0.*** ***Неудовлетворительно – менее 50% правильных ответов*** ***Удовлетворительно - от 51% правильных ответов.*** ***Хорошо - от 70%.***
Согласно учебному плану	тестирование	ПК-1 ПК-3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением.*** ***Неявка – 0.*** ***Неудовлетворительно – менее 50% правильных ответов*** ***Удовлетворительно - от 51% правильных ответов.*** ***Хорошо - от 70%.***
Согласно учебному плану	Зачет	ПК-1 ПК-3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки: **«Зачтено»:** 1. знание лексического и грамматического материала; 2. умение использовать и применять 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.

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

4.1. Типовые вопросы, выносимые на тестирование

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

1. 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?

4.2. 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

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)

ОСНОВЫ РЭБ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль): Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев

2023

1. Общие положения

Цель дисциплины:

- 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.

Задачи дисциплины:

- формирование у студентов базовых знаний в области радиотехнического контроля информационных систем.
- практическое ознакомление с современными техническими средствами радиотехнического контроля информационных систем.

2. Указания по проведению практических занятий

Практическое занятие 1.

Тема: Сущность и содержание радиотехнического контроля

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

Образовательные технологии: *групповая дискуссия.*

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: 6 ч.

Практическое занятие 2.

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

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

Образовательные технологии: *беседа*.

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:6 ч.

Практическое занятие 3

Тема: Основы организации радиотехнического контроля функционирования информационных систем

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

Образовательные технологии: *беседа.*

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: 6 ч.

Практическое занятие 4

Тема: Базовые технологии обеспечения радиоэлектронной безопасности функционирования информационных систем

Вид практического занятия**:** *подготовка реферата.*

Образовательные технологии: *практическая работа по группам.*

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: 6 ч.

3. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Раздел 1. Основы технического контроля Функционирования радиоэлектронных систем и средств	***Подготовка рефератов, письменная работа, самостоятельное изучение тем.*** Примерная тематика ***рефератов (докладов, письменных работ и т.д.): … (разрабатывается самостоятельно преподавателем на основе рабочей программы).*** 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. 5. методы и средства радионаблюдения; 6. типовая структура радиотехнического канала утечки информации; .
2.	Раздел 2. Организация и технологии радиоэлектронной защиты современных информационных систем.	***Подготовка рефератов, письменная работа, самостоятельное изучение тем, работа с программным обеспечением, создание презентаций.*** Примерная тематика ***рефератов (докладов, письменных работ и т.д.): … (разрабатывается самостоятельно преподавателем на основе рабочей программы).*** 7. основные показатели радиотехнических каналов утечки информации; 8. простые и составные каналы утечки информации;

		9. радиоэлектронный канал утечки информации; 10. материально-вещественный канал утечки информации; 11. методы и средства защиты информации от подслушивания; 12. методы и средства защиты информации от наблюдения; 13. методы и средства защиты информации от перехвата; 14. методы и средства контроля защищенности информации от утечки по техническим каналам.
3.	Введение. Основные понятия теории компьютерной безопасности	***Подготовка докладов и презентаций по темам:*** Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
4	Анализ угроз информационной безопасности для компьютерных систем	***Подготовка докладов и презентаций по темам:*** Классификация компьютерных систем, подлежащих защите в зависимости от обрабатываемой информации и функционального назначения. Классификация СВТ по уровню защищённости от НСД к информации. Перечень показателей защищённости СВТ и совокупности описывающих их требований. Характеристика классов защищённости СВТ от НСД к информации. Виды и анализ угроз автоматизированных систем, компьютерные вирусы, технология и способы вторжения в устойчивую работу автоматизированных систем злоумышленников. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
5	Основные уровни защиты информации в компьютерных системах	***Подготовка докладов и презентаций по темам:*** Классификация АС, подлежащих защите от НСД к информации. Требования по защите информации в АС различных классов. Этапы классификации АС. Исходные данные для классификации АС. Выбор класса защищённости АС.

		Структура документации системы менеджмента информационной безопасности в организации. Модель PDCA. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.* Алгоритм и матрица оценки рисков при обеспечении информационной безопасности в организации. Варианты обработки рисков. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
6	Основные положения формальной теории защиты информации	***Подготовка докладов и презентаций по темам:*** Перечень основных документов ФСТЭК России по вопросам защиты информации. Система разграничения доступа (СРД) и её функции. Средства для СРД. Реализация СРД. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
7	Формальные модели безопасности	***Подготовка докладов и презентаций по темам:*** Построение модели нарушителя безопасности АС. Уровни возможностей, предоставляемые нарушителям штатными средствами АС и СВТ. Базовая модель угроз ИСПДн. Модель распространения прав доступа Take-Grant. Цель использования модели Take-Grant. Основные элементы модели Take-Grant. Формальное описание модели Take-Grant. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
8	Концептуальные положения системы менеджмента информационной безопасности применительно к компьютерным системам	***Подготовка докладов и презентаций по темам:*** Лицензирование и сертификация в области защиты информации. Комплексные системы защиты информации. Аттестация АС по требованиям безопасности информации. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
	Построение систем защиты от угрозы нарушения конфиденциальности, целостности и доступности компьютерной	***Подготовка докладов и презентаций по темам:*** Описание систем защиты с помощью матрицы доступа. Таблицы, описывающие права доступа субъектов к объектам. Описание модели Харрисона-Руззо-Ульмана (HRU). Сущность построения системы защиты информации. Оптимальные механизмы обеспечения защиты информации

	информации	и механизмы управления. Выбор способа постановки задачи. Методы построения защищённых АС. Принципы проектирования. Структурный принцип и принцип модульного проектирования. Три основных конструкции для проектирования. Преимущества использования модульного принципа. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*

4. Указания по проведению контрольных работ

Контрольные работы не предусмотрены учебным планом.

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

Основная литература:

1.Овсянников, С. В.Проектирование систем наведения радиотехнических и оптических комплексов. Ч. 2 : учеб. пособие по курсу «Проектирование мехатронных систем» / Овсянников С. В. - М. : Изд-во МГТУ им. Н.Э. Баумана, 2009. - 48 : нет. - ISBN ----. - Электронная программа (визуальная). Электронные данные : электронные.
URL: https://lib.rucont.ru/efd/287519

2.Стасенко, И. В.Радиоэлектронные системы и устройства / Стасенко И. В. - М. : Изд-во МГТУ им. Н.Э. Баумана, 2013. - 44 : нет. - ISBN 978-5-7038-3685-9. - Электронная программа (визуальная). Электронные данные : электронные.
URL: https://lib.rucont.ru/efd/287592

3.Статистический анализ и синтез радиотехнических устройств и систем: учебное пособие для вузов / В. И. Тихонов, В.Н. Харисов. — М.: Горячая линия-Телеком, 2014. — 608 с.

Дополнительная литература:

4.Электродинамика и распространение радиоволн : учебное пособие / Д.Ю. Муромцев, Ю.Т. Зырянов, П.А. Федюнин и др. – Тамбов : Изд-во ФГБОУ ВПО «ТГТУ», 2012. – 200 с

5.Теория оптимальных методов радиоприема при флуктуационных помехах / Л.С. Гуткин. — М.: Сов. радио, 1972. — 447 с.

Теоретические основы радиолокации и радионавигации: Учеб. пособие для радиотехн. спец. вузов / Ю. Г. Сосулин. — М.: Радио и связь, 1992. — 303 с.

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

Интернет-ресурсы:

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

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

Перечень программного обеспечения: *MSOffice, PowerPoint.*

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета
2. Рабочая программа и методическое обеспечение по дисциплине «Основы РЭБ в 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/)..