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)

Б.1.В.ДВ.09.02 «ОСНОВЫ РАДИОЭЛЕКТРОННОЙ РАЗВЕДКИ (РЭР)»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

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 радиоэлектронной разведки (РЭР)». – Королев МО: «Технологический университет», 2023.

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 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2023	2024	2025	2026
Номер и дата протокола заседания кафедры	№8 от 29.03.2023			

Рабочая программа согласована:

Руководитель ОПОП ВО Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024	2025	2026
Номер и дата протокола заседания УМС	№5 от 11.04.2023			

2

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 радиоэлектронной разведки.

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 радиоэлектронной разведки
2. Практическое ознакомление с современными техническими средствами радиоэлектронной разведки.

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 «Основы радиоэлектронной разведки (РЭР)» 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» и компетенциях: ОПК-2,3,4,11; УК-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			
ОЧНО-ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	28			28	
Лекции (Л)	12			12	
Практические занятия (ПЗ)	16			16	
Лабораторные работы (ЛР)	-			-	
Самостоятельная работа	80			80	
Другие виды контактной работы	**10**			10	
Курсовые работы (проекты)	-			-	
Расчетно-графические работы	-			-	
Контрольная работа, домашнее задание	+ -			+ -	
Практическая подготовка				-	
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/заочное	Практические занятия, час. очное/заочное	Занятия в интерактивной форме, час. очное/заочное	Код компетенций
1	2	3	4	5
Раздел 1. Основные демаскирующие признаки радиоэлектронных объектов, привлекаемые силы (средства) и возможности радиоэлектронной разведки				
Тема 1. Демаскирующие признаки функционирования радиоэлектронных объектов информационных систем и основные положения по радиоэлектронной разведки	4/3	8/3	-/1	ПК-3
Тема 2. Привлекаемые силы (средства), виды и особенности ведения радиоэлектронной разведки	4/3	8/3	-/3	ПК-3
Раздел 2. Аналитико-информационное обеспечение радиоэлектронной безопасности функционирования информационных объектов				
Тема 3. **Оценка радиоэлектронной обстановки на защищаемых информационных объектах**	4/3	8/3	-/3	ПК-5
Тема 4. **Основы обоснования целесообразных мер по радиоэлектронной защите информационных объектов**	4/3	8/7	-/3	ПК-5
	16/12	32/16	-/10	

4.2. Содержание тем дисциплины

Раздел 1. Основные демаскирующие признаки радиоэлектронных объектов, привлекаемые силы (средства) и возможности радиоэлектронной разведки

Тема 1. Демаскирующие признаки функционирования радиоэлектронных объектов информационных систем и основные положения по радиоэлектронной разведки

Сущность и классификация основных демаскирующих признаков функционирования радиоэлектронных объектов в информационных системах.

Общая характеристика радиоэлектронной разведки. Использование радиочастот в радиоэлектронной разведки. Приемные антенны, аппаратура поиска, перехвата, пеленгации и анализа радиосигналов в системах радиоэлектронной разведки.

Тема 2. Привлекаемые силы (средства), виды и особенности ведения радиоэлектронной разведки

Современные силы и средства радиоэлектронной разведки, способы их применения. Основы радио и радиотехнической, радиолокационной разведок.

Назначение и задачи радиотехнической разведки (РТР). Блок схема станции РТР. Способы определения и запоминания частот излучения разведываемых РЭС. Определение местонахождения и опознавания работающих РЭС.

Раздел 2. Аналитико-информационное обеспечение радиоэлектронной безопасности функционирования информационных объектов

Тема 3. Оценка радиоэлектронной обстановки на защищаемых информационных объектах

Выявление наиболее опасных потенциальных и реальных источников и видов информационных угроз для радиоэлектронных объектов. Основы прогнозирования и расчеты по анализу радиоэлектронной обстановки. Определение наиболее уязвимых радиоэлектронных объектов.

Тема 4. Основы обоснования целесообразных мер по радиоэлектронной защите информационных объектов

Состав и характеристика целесообразных мер по радиоэлектронной защите радиоэлектронных объектов от различных видов радиоэлектронной разведки.

Общие положения по устранению или ослаблению электромагнитных воздействий на свои радиоэлектронные объекты.

Маскировка и незаметность функционирования своих радиоэлектронных систем и средств. Способы обеспечения радио незаметности. Снижение радиолокационной незаметности. Маскирующее воздействие на среду распространения радиосигналов.

Помехозащита радиоприемных устройств. Радиоэлектронная защита радиолокационных станций. Помехозащита радиосистем передачи информации. Радиоэлектронная защита систем радиоуправления ракетами.

Защита своих радиоэлектронных объектов от поражения самонаводящимися на излучение оружием.

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 «Выработка политики информационной безопасности», приведена в Приложении 1.

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

Основная литература:

1.Перунов, Ю. М. Радиоэлектронная борьба в информационных каналах : монография / Ю. М. Перунов, А. И. Куприянов. — Вологда : Инфра-Инженерия, 2021. — 452 с. — ISBN 978-5-9729-0718-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/192374 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

2.Трухин, М. П. Основы компьютерного проектирования и моделирования радиоэлектронных средств : учебное пособие / М. П. Трухин. — Москва : Горячая линия-Телеком, 2017. — 386 с. — ISBN 978-5-9912-0449-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111111 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

3.Дмитриев, В. Г. Радиоэлектронная борьба: функциональное поражение радиоэлектронных средств : монография / В. Г. Дмитриев. — Вологда : Инфра-Инженерия, 2021. — 268 с. — ISBN 978-5-9729-0700-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/192376 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

4.Елисеев, С. Н. Конспект лекций по учебной дисциплине Основы теории систем и комплексов радиоэлектронной борьбы. По специальности (направлению подготовки): 11.05.01 Радиоэлектронные системы и комплексы : учебное пособие / С. Н. Елисеев. — Самара : ПГУТИ, 2018. — 95 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182195 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

5.Куприянов, А. И. Теоретические основы радиоэлектронной разведки : учебное пособие / А. И. Куприянов, П. Б. Петренко, М. П. Сычев. — Москва :

МГТУ им. Баумана, 2010. — 381 с. — ISBN 978-5-7038-3325-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/106536 (дата обращения: 23.12.2022). — Режим доступа: для авториз. пользователей.

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. Электронные ресурсы образовательной среды Университета.
2. Рабочая программа и методическое обеспечение по дисциплине: «Основы радиоэлектронной разведки (РЭР)»
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

«ОСНОВЫ РАДИОЭЛЕКТРОННОЙ РАЗВЕДКИ (РЭР)»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

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

№ п/п	Индекс компе-тенции	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 высоком уровне) – 90% правильных ответов* *Б) частично сформирована:* • *компетенция освоена на продвинутом уровне – 70% правильных ответов;* • *компетенция освоена на базовом уровне – от 51% правильных ответов;* *В) не сформирована (компетенция не сформирована) – 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 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:* *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 информационных объектов по акустическому каналу;
2. современные комплексы контроля защищенности информационных объектов по виброакустическому каналу;
3. технические средства поиска пустот и принцип их действия;
4. технические средства поиска металлических изделий и принцип их работы;
5. нелинейные локаторы;
6. принципы работы и разновидности индикаторов поля;
7. технические средства контроля телефонных линий;
8. технические средства контроля радиоэлектронной обстановки;
9. технические средства локализации радиоизлучающих закладных устройств.

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

Формой контроля знаний по дисциплине «Основы радиоэлектронной разведки (РЭР)» являются две текущие аттестации в виде тестов и одна итоговая аттестация в форме 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 разведкой?
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 разведки?
11. Основные задачи радиоэлектронной разведки?
12. Что называют перехватом?
13. Основные функции радиоэлектронной разведки?
14. Что понимают под основными техническими средствами и системами?
15. Субъекты радиоэлектронной разведки?
16. Что называют каналом утечки информации?
17. Оценка радиоэлектронной разведки?
18. Укажите правильный перечень технических каналов утечки информации?

19. Основные мероприятия по обеспечению радиоэлектронной разведки?
20. Какой из показателей не является показателем технического канала утечки информации?

Типовые вопросы, выносимые на зачет.

1. Радиоэлектронная обстановка. Виды РЭО. Сущность и методика оценки РЭО.
2. Радиоэлектронная борьба. Составные части РЭБ. Сущность, цели и задачи радиоэлектронной борьбы.
3. Радиоэлектронная разведка. Составные части РЭР. Сущность, цели и задачи.
4. Радиоэлектронное поражение. Составные части РЭП. Сущность, цели и задачи.
5. Радиоэлектронная защита. Составные части РЭЗ. Сущность, цели и задачи.
6. Радиоэлектронно-информационное обеспечение. Составные части РИО. Сущность, цели и задачи.
7. Назначение комплекса «Мандат», основные характеристики входящих в него средств.
8. Возможности комплекса «Мандат» и методика их расчёта.
9. Варианты построения базового комплекса радио подавления. Режимы работы АПУ и АСП.
10. Размещение средств комплекса «Мандат» на местности. Организация связи между средствами комплекса.
11. Назначение, организационно-штатная структура, вооружение и боевые возможности ор РЭБ мсбр (тбр).
12. Назначение, организационно-штатная структура, вооружение и боевые возможности об РЭБ мсбр (тбр).
13. Задачи частей и подразделений РЭБ в бою (операции).
14. Боевые порядки частей и подразделений РЭБ. Порядок выбора позиции АСП.
15. Действия частей и подразделений РЭБ при ведении радиоразведки и создании радиопомех. Способы боевого применения частей и подразделений РЭБ.
16. Система управления и связи части РЭБ. Способы управления подразделениями.
17. Методы, содержание и последовательность работы командира части РЭБ по организации боевого применения.
18. Порядок принятия командиром части РЭБ решения на боевое применение.
19. Оперативно-тактические расчёты. Порядок ведения рабочей карты.
20. Виды боевого, технического и тылового обеспечения их содержание.
21. Классификация демаскирующих признаков
22. Понятие о демаскирующих объектах, сигналах и веществах.
23. Виды носителей информации
24. Способы записи информации на различные виды носителей
25. Принципы съема информации путем демодуляции (детектирования)
26. Источники опасных сигналов
27. Виды угроз безопасности информации

28. Факторы, влияющие на возможность реализации угроз безопасности информации
29. Виды зарубежной разведки и разведки коммерческих структур
30.Классификация технической разведки
31.Основные принципы и этапы добывания информации
32.Принципы идентификации и интерпретации, обнаружения и распознавания объектов, измерения характеристик демаскирующих признаков
33.Принципы доступа к источникам информации без физического проникновения в контролируемую зону
34.Классификация и характеристики наземных средств дистанционного съема информации с носителей
35.Возможности зарубежной космической, воздушной и морской разведки в мирное время
36.Типовая структура технического канала утечки информации.
37.Оптические каналы утечки информации и их особенности
38.Радиоэлектронные каналы утечки информации и их особенности
39.Акустические каналы утечки информации и их особенности
40.Материально-вещественные каналы утечки информации и их особенности
41.Сущность инженерной защиты и технической охраны источников информации
42.Показатели эффективности инженерно-технической защиты информации
43.Концепция охраны объектов. Типовая структура системы охраны
44.Способы и средства инженерной защиты объектов
45.Способы и средства обнаружения злоумышленников и пожара
46.Способы и средства видеоконтроля
47.Средства управления системой охраны объектов
48.Способы и средства противодействия наблюдению в оптическом диапазоне длин волн
49.Способы и средства противодействия радиолокационному наблюдению
50.Способы и средства информационного скрытия акустических сигналов и речевой информации
51.Способы и средства энергетического скрытия акустических сигналов
52.Способы и средства предотвращения утечки информации с помощью закладных устройств
53.Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки
54.Классификация способов предотвращения утечки информации по материально-вещественному каналу
55.Краткая характеристика государственной системы защиты информации
56.Понятие о моделировании как основном процессе системного анализа
57.Моделирование объектов защиты
58.Моделирование угроз информации
59.Задачи и виды контроля эффективности защиты информации.
60.Функции сотрудников службы безопасности, обеспечивающих инженерно-техническую защиту информации

61.Методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам.
62.Методика оценки утечки информации за счет акустоэлектрических преобразований в ВТСС.
63.Методика оценки утечки информации от ОТСС за счет ПЭМИН

**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)

«ОСНОВЫ РАДИОЭЛЕКТРОННОЙ РАЗВЕДКИ (РЭР)»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

1. Общие положения

Целями изучения дисциплины является:

– формирование у студентов базовых знаний и практических навыков в области радиоэлектронной разведки.

– ознакомление студентов с современными средствами защиты информации и радиоэлектронной разведки.

Задачами дисциплины являются:

1. Формирование у студентов базовых знаний в области радиоэлектронной разведки
2. Практическое ознакомление с современными техническими средствами радиоэлектронной разведки.

2. Указания по проведению практических занятий

Практическое занятие 1.

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

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

Тема. Демаскирующие признаки функционирования радиоэлектронных объектов информационных систем и основные положения по радиоэлектронной разведки

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

Тема и содержание практического занятия:

Цель работы: Получить практические умения демаскирующих признаков функционирования радиоэлектронных объектов информационных систем.

Основные положения темы занятия:

1. Сущность и классификация основных демаскирующих признаков функционирования радиоэлектронных объектов в информационных системах.
2. Общая характеристика радиоэлектронной разведки. Использование радиочастот в радиоэлектронной разведки. Приемные антенны, аппаратура поиска, перехвата, пеленгации и анализа радиосигналов в системах радиоэлектронной разведки.

Вопросы для обсуждения:

1. Классификация радиосистем в целом и радиолокационных систем
2. Классификация радионавигационных систем и методы определения навигационных параметров
3. Отражающие свойства объектов.
4. Дальность действия радиолинии (пассивной радиосистемы)
5. Дальность действия активной радиолокационной системы
6. Дальность действия полуактивной радиосистемы и радиосистемы с

активным ответом

Продолжительность занятия: 4/2 ч.

Практическое занятие 2.

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

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

Тема. Привлекаемые силы (средства), виды и особенности ведения радиоэлектронной разведки

.

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

Тема и содержание практического занятия:

Цель работы: Получить практические знания привлекаемых сил (средства), видов и особенности ведения радиоэлектронной разведки

Основные положения темы занятия:

1. Современные силы и средства радиоэлектронной разведки, способы их применения. Основы радио и радиотехнической, радиолокационной разведок.
2. Назначение и задачи радиотехнической разведки (РТР). Блок схема станции РТР. Способы определения и запоминания частот излучения разведываемых РЭС. Определение местонахождения и опознавания работающих РЭС.

Вопросы для обсуждения:

1. Влияние Земли на дальность действия радиосистем
2. Влияние атмосферы на дальность действия радиосистем
3. Виды АМ модуляторов.
4. Классификация СПИ (системы перехвата информации).
5. Селекция движущихся целей.
6. АМ-ПН сигнал и его спектр. Модуляция и демодуляция.
7. Асинхронные многоканальные СПИ.
8. Виды модуляции. Информативные и неинформативные параметры сигнала.
9. Синхронизация в СПИ с современным разделением каналов.
10. Взаимодействие человека и РЭА на этапах ее разработки и эксплуатации.
11. Методы борьбы с замираниями сигналов.
12. Система связи с обратным каналом.
13. Модель распространения радиоволн.

Продолжительность занятия: 4/2 ч.

Практическое занятие 3

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

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

Тема. Оценка радиоэлектронной обстановки на защищаемых

информационных объектах

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки оценки радиоэлектронной обстановки на защищаемых информационных объектах.

Основные положения темы занятия:

1. Выявление наиболее опасных потенциальных и реальных источников и видов информационных угроз для радиоэлектронных объектов.
2. Основы прогнозирования и расчеты по анализу радиоэлектронной обстановки. Определение наиболее уязвимых радиоэлектронных объектов.

Вопросы для обсуждения:

1. Методы сжатия информации, их классификация.
2. Формула дальности действия систем связи и радиолокации.
3. Автономное управление объекта.
4. Избыточность источника сообщений. Статистическое кодирование, как метод устранения избыточности.
5. Примеры согласованных фильтров для одиночных импульсов и их пачки.
6. Методы наведения управляемых объектов.
7. Классификация кодов.
8. Типы управляемых объектов. Системы координат и управление движения.
9. Квантование сигналов по уровню. Коды, их характеристики.
10. Обнаружение сигнала с неизвестной фазой. Структура оптимального обнаружителя.
11. Методы радионаведения.
12. Ошибки дискретизации непрерывных сообщений

Продолжительность занятия: 4/2 ч.

Практическое занятие 4

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

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

Тема. Основы обоснования целесообразных мер по радиоэлектронной защите информационных объектов

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки обоснования целесообразных мер по радиоэлектронной защите информационных объектов.

Основные положения темы занятия:

1. Состав и характеристика целесообразных мер по радиоэлектронной защите радиоэлектронных объектов от различных видов

радиоэлектронной разведки.
2. Общие положения по устранению или ослаблению электромагнитных воздействий на свои радиоэлектронные объекты.
3. Маскировка и незаметность функционирования своих радиоэлектронных систем и средств. Способы обеспечения радио незаметности. Снижение радиолокационной незаметности. Маскирующее воздействие на среду распространения радиосигналов.
4. Помехозащита радиоприемных устройств. Радиоэлектронная защита радиолокационных станций. Помехозащита радиосистем передачи информации. Радиоэлектронная защита систем радиоуправления ракетами.
5. Защита своих радиоэлектронных объектов от поражения самонаводящимися на излучение оружием.

Вопросы для обсуждения:

1. Два вида дискретизации непрерывных сообщений. Теорема Котельникова.
2. Обнаружение сигналов как статистическая задача. Критерий обнаружения. Отношение правдоподобие.
3. Характеристики эффективности обнаружения
4. Основные тактико-технические характеристики РЛС.
5. Прогнозирование отказов, выбор частоты и объема проверок.
6. Электронный и оптический методы обработки информации.
7. Диапазоны радиоволн, влияние условий их распространения на работу РЛ и РН.
8. Космические радиолинии.
9. Структура аналогового и цифрового не следящего амплитудного пеленгатора.
10. Опознавание и распознавание объектов

Продолжительность занятия: 4/2 ч.

3. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	**Тема 1. Демаскирующие признаки функционирования радиоэлектронных объектов информационных систем и основные положения по радиоэлектронной разведки**	***Подготовка докладов по темам:*** 1. . современные комплексы контроля защищенности информационных объектов по акустическому каналу; 2. современные комплексы контроля защищенности информационных объектов по виброакустическому каналу; 3. современные комплексы контроля защищенности информационных объектов по радиоэлектронному каналу. 4. принципы записи и съема информации с ее

		носителя; 5. методы и средства подслушивания;
2.	**Тема 2. Привлекаемые силы (средства), виды и особенности ведения радиоэлектронной разведки**	***Подготовка докладов по темам:*** 1. методы и средства наблюдения; 2. методы и средства перехвата; 3. методы и средства физико-химического анализа; 4. типовая структура технического канала утечки информации; 5. основные показатели технических каналов утечки информации; 6. простые и составные каналы утечки информации; 7. акустический канал утечки информации;
3	***Тема 3.*** **Оценка радиоэлектронной обстановки на защищаемых информационных объектах**	***Подготовка докладов по темам:*** 1. визуально-оптический канал утечки информации; 2. радиоэлектронный канал утечки информации; 3. материально0вещественный канал утечки информации; 4. методы и средства защиты информации от подслушивания; 5. методы и средства защиты информации от наблюдения; 6. методы и средства защиты информации от перехвата; 7. методы и средства контроля защищенности информации от утечки по техническим каналам.
4	***Тема 4.*** **Основы обоснования целесообразных мер по радиоэлектронной защите информационных объектов**	***Подготовка докладов по темам:*** 1.Методы поиска и локализации излучающих закладных устройств. 2. Методы поиска и локализации неизлучающих закладных устройств. 3. Средства поиска и локализации излучающих закладных устройств. 4. Средства поиска и локализации неизлучающих закладных устройств. 5. Методика проведения специальных исследований защищенности информационного объекта от подслушивания 6. Методика проведения специальных исследований защищенности информационного объекта от утечки по радиоэлектронному каналу

5. Указания по проведению контрольных работ

5.1. Требование к структуре

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

5.2. Требование 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.

5.3. Требования к оформлению

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

5.4. Примерная тематика контрольных работ:

1. Радиоэлектронная обстановка. Виды РЭО. Сущность и методика оценки РЭО.
2. Радиоэлектронная борьба. Составные части РЭБ. Сущность, цели и задачи радиоэлектронной борьбы.
3. Радиоэлектронная разведка. Составные части РЭР. Сущность, цели и задачи.
4. Радиоэлектронное поражение. Составные части РЭП. Сущность, цели и задачи.
5. Радиоэлектронная защита. Составные части РЭЗ. Сущность, цели и задачи.
6. Радиоэлектронно-информационное обеспечение. Составные части РИО. Сущность, цели и задачи.
7. Назначение комплекса «Мандат», основные характеристики входящих в него средств.
8. Возможности комплекса «Мандат» и методика их расчёта.
9. Варианты построения базового комплекса радио подавления. Режимы работы АПУ и АСП.

10. Размещение средств комплекса «Мандат» на местности. Организация связи между средствами комплекса.
11. Назначение, организационно-штатная структура, вооружение и боевые возможности ор РЭБ мсбр (тбр).
12. Назначение, организационно-штатная структура, вооружение и боевые возможности об РЭБ мсбр (тбр).
13. Задачи частей и подразделений РЭБ в бою (операции).
14. Боевые порядки частей и подразделений РЭБ. Порядок выбора позиции АСП.
15. Действия частей и подразделений РЭБ при ведении радиоразведки и создании радиопомех. Способы боевого применения частей и подразделений РЭБ.
16. Система управления и связи части РЭБ. Способы управления подразделениями.
17. Методы, содержание и последовательность работы командира части РЭБ по организации боевого применения.
18. Порядок принятия командиром части РЭБ решения на боевое применение.
19. Оперативно-тактические расчёты. Порядок ведения рабочей карты.
20. Виды боевого, технического и тылового обеспечения их содержание.
21. Классификация демаскирующих признаков
22. Понятие о демаскирующих объектах, сигналах и веществах.
23. Виды носителей информации
24. Способы записи информации на различные виды носителей
25. Принципы съема информации путем демодуляции (детектирования)
26. Источники опасных сигналов
27. Виды угроз безопасности информации
28. Факторы, влияющие на возможность реализации угроз безопасности информации
29. Виды зарубежной разведки и разведки коммерческих структур
30.Классификация технической разведки
31.Основные принципы и этапы добывания информации
32.Принципы идентификации и интерпретации, обнаружения и распознавания объектов, измерения характеристик демаскирующих признаков
33.Принципы доступа к источникам информации без физического проникновения в контролируемую зону
34.Классификация и характеристики наземных средств дистанционного съема информации с носителей
35.Возможности зарубежной космической, воздушной и морской разведки в мирное время
36.Типовая структура технического канала утечки информации.
37.Оптические каналы утечки информации и их особенности
38.Радиоэлектронные каналы утечки информации и их особенности
39.Акустические каналы утечки информации и их особенности
40.Материально-вещественные каналы утечки информации и их особенности
41.Сущность инженерной защиты и технической охраны источников

информации
42.Показатели эффективности инженерно-технической защиты информации
43.Концепция охраны объектов. Типовая структура системы охраны
44.Способы и средства инженерной защиты объектов
45.Способы и средства обнаружения злоумышленников и пожара
46.Способы и средства видеоконтроля
47.Средства управления системой охраны объектов
48.Способы и средства противодействия наблюдению в оптическом диапазоне длин волн
49.Способы и средства противодействия радиолокационному наблюдению
50.Способы и средства информационного скрытия акустических сигналов и речевой информации
51.Способы и средства энергетического скрытия акустических сигналов
52.Способы и средства предотвращения утечки информации с помощью закладных устройств
53.Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки
54.Классификация способов предотвращения утечки информации по материально-вещественному каналу
55.Краткая характеристика государственной системы защиты информации
56.Понятие о моделировании как основном процессе системного анализа
57.Моделирование объектов защиты
58.Моделирование угроз информации
59.Задачи и виды контроля эффективности защиты информации.
60.Функции сотрудников службы безопасности, обеспечивающих инженерно-техническую защиту информации
61.Методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам.
62.Методика оценки утечки информации за счет акустоэлектрических преобразований в ВТСС.
63.Методика оценки утечки информации от ОТСС за счет ПЭМИН

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

Основная литература:

1. Радиотехнические системы/ Под ред. Ю.М. Казаринова. – М.: Академия, 2008. 2.
2. Борисов В.И. и др. Помехозащищенность систем радиосвязи. – М.: Радиотехника, 2010.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).

9. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice, PowerPoint.*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды Университета.
2. Рабочая программа и методическое обеспечение по дисциплине «Основы радиоэлектронной разведки (РЭР)».
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/)..