ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Утверждено
на заседании кафедры
протокол № 6 от 31 января 2022 г.
Зав. кафедрой _____ / Исмагилова А.С.

Согласовано
Председатель УМК института


/ Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Техническая радиоэлектронная разведка

Часть, формируемая участниками образовательных отношений

программа бакалавриата

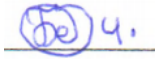
Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль) подготовки
Организация и технологии защиты
(в системе государственного и муниципального управления)

Квалификация
Бакалавр

Форма обучения
Очная

Разработчик (составитель)
Ассистент


/ Белова Е. П.

Для приема 2022 г.

Уфа - 2022 г.

Составитель: Белова Елена Петровна

Рабочая программа дисциплины утверждена на заседании кафедры управления информационной безопасностью, протокол № 6 от 31 января 2022 г.

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций
2. Цель и место дисциплины в структуре образовательной программы
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)
4. Фонд оценочных средств по дисциплине

   4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

   4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине.
5. Учебно-методическое и информационное обеспечение дисциплины

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

   5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций (при наличии ОПК)	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
	ПК-2 Способен управлять защитой информации в автоматизированных системах.	*ПК 2.1. Знать методы защиты информации в автоматизированных системах.*	*Знает методы защиты информации в автоматизированных системах.*
		ПК 2.2 Уметь управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.	*Умеет управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.*
		ПК 2.3 Владеть навыками выявления и анализа уязвимостей, выбора оптимальной стратегии для обеспечения информационной безопасности в автоматизированных системах.	*Владеет навыками выявления и анализа уязвимостей, выбора оптимальной стратегии для обеспечения информационной безопасности в автоматизированных системах.*

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Техническая радиоэлектронная разведка» относится к части, формируемой участниками образовательных отношений.
Дисциплина изучается на 4 курсе в 1 семестре..
Целью учебной дисциплины «Техническая радиоэлектронная разведка» является изучение основных принципов работы радиоэлектронных средств, применяемых в радиоэлектронной разведке, получение навыков выбора метода для успешного осуществления разведывательной деятельности и её обнаружения.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

ПК-2 - Способен управлять защитой информации в автоматизированных системах.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК 2.1 - Знать методы защиты информации в автоматизированных системах.	Знать методы защиты информации в автоматизированных системах.	Не знает методы защиты информации в автоматизированных системах.	Имеет отдалённые представления о методах защиты информации в автоматизированных системах.	Частично знает методы защиты информации в автоматизированных системах.	Знает методы защиты информации в автоматизированных системах.
ПК 2.2 - Уметь управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.	Уметь управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.	Не умеет управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.	Имеет отдалённые представления об управлении специализированным программным обеспечением для защиты информации в автоматизированных системах.	Частично умеет управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.	Умеет управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.
ПК 2.3 - Владеть навыками выявления и анализа уязвимост	Владеть навыками выявления и анализа уязвимостей, выбора оптимальной	Не владеет навыками выявления и анализа уязвимостей, выбора оптимальной	Имеет смутные представления о выявлении и анализе уязвимостей,	Частично владеет навыками выявления и анализа уязвимостей, выбора	Владеет навыками выявления и анализа уязвимостей, выбора оптимальной

ей, выбора оптимальной стратегии для обеспечения информационной безопасности в автоматизированных системах.	стратегии для обеспечения информационной безопасности в автоматизированных системах.	стратегии для обеспечения информационной безопасности в автоматизированных системах.	выборе оптимальной стратегии для обеспечения информационной безопасности в автоматизированных системах.	оптимальной стратегии для обеспечения информационной безопасности в автоматизированных системах.	стратегии для обеспечения информационной безопасности в автоматизированных системах.

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей, перечисленных в рейтинг-плане дисциплины (для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания для экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Оценочные средства
ПК-2 Способен управлять защитой информации в автоматизированных системах.	Знать методы защиты информации в автоматизированных системах.	Аудиторная работа, тесты, устный опрос.
	Уметь управлять специализированным программным обеспечением для защиты информации в автоматизированных системах.	Аудиторная работа, тесты, устный опрос.
	Владеть навыками выявления и анализа уязвимостей, выбора оптимальной стратегии для обеспечения информационной	Аудиторная работа, тесты, устный опрос.

	безопасности в автоматизированных системах.	

Рейтинг-план
дисциплины «Техническая радиоэлектронная разведка»

Виды учебной деятельности	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Радиоэлектронная разведка				
Текущий контроль			**0**	35
1. Аудиторная работа	5	6	0	30
2. Устный опрос	1	5	0	5
Рубежный контроль			**0**	10
1.Тесты	1	10	0	10
Модуль 2. Радиоэлектронное подавление РЭС, скрытность и помехозащита РЭС				
Текущий контроль			**0**	35
1. Аудиторная работа	5	6	0	30
2. Устный опрос	1	5	0	5
Рубежный контроль			**0**	10
1.Тесты	1	10	0	10
Поощрительные баллы				
1. Студенческая олимпиада, участие в конференциях	5			5
2. Публикация статей	5			5
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
Посещение лекционных занятий			0	–6
2. Посещение практических (семинарских, лабораторных занятий)			0	–10
Итоговый контроль				
Экзамен			0	30

Устный индивидуальный опрос

Устный индивидуальный опрос проводится после изучения новой темы с целью выяснения наиболее сложных вопросов, степени усвоения информации.

Обучающийся излагает содержание вопроса изученной темы.

Критерии и методика оценивания:

- 5 баллов выставляется обучающемуся, если точно используется специализированная терминология, показано уверенное владение нормативной базой;

- 4 балла выставляется обучающемуся, допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология;

- 3 балла выставляется обучающемуся, нет общего понимания вопроса, имеются

затруднения или допущены ошибки в определении понятий, использовании терминологии.

Устный групповой опрос

Устный групповой опрос проводится после изучения новой темы с целью выяснения наиболее сложных вопросов, степени усвоения информации, поддержания внимания слушающей аудитории.

Критерии и методика оценивания:

- 5 баллов выставляется обучающемуся, если точно используется специализированная терминология, показано уверенное владение нормативной базой;

- 4 балла выставляется обучающемуся, допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология;

- 3 балла выставляется обучающемуся, нет общего понимания вопроса, имеются затруднения или допущены ошибки в определении понятий, использовании терминологии

Экзамен

Проводится в 7 семестре. Экзаменационный билет содержит 2 теоретических вопроса.

Типовые экзаменационные вопросы:

1. Актуальность проблемы борьбы с технической радиоэлектронной разведкой.
2. Проблемы создания инструментального базиса защиты информации.
3. Криминалистическая характеристика преступлений, связанных с осуществлением технической радиоэлектронной разведки.
4. Организационная и техническая защита информации от утечки по техническим каналам.
5. Криминалистическая характеристика преступлений в сфере компьютерной информации.
6. Способы и средства защиты компьютерной информации от технической радиоэлектронной разведки.
7. Объекты, элементы и средства защиты информации в компьютерных системах обработки данных.
8. Средства опознания санкционированных пользователей и разграничения доступа к информации.
9. Криптографический метод защиты информации.
10. Особенности защиты программных продуктов.
11. Особенности организационной и технической защиты информации, обрабатываемой средствами вычислительной техники.
12. Правовая защита от компьютерных преступлений.
13. Миниатюрные телекамеры и их объективы, портативные видеопередатчики, ретрансляторы и приемники телевизионного сигнала, средства дистанционного управления аппаратурой, предметы прикрытия (камуфляжа) телекамер.
14. Приборы ночного видения.
15. Миниатюрные, остронаправленные микрофоны, стетоскопы, лазерные системы аудиоконтроля.
16. Магнитофоны, диктофоны и бескинематические средства звукозаписи.
17. Миниатюрные радиопередающие устройства, цифровые закрытые радиолинии передачи акустических сигналов, радиомикрофоны с дистанционным управлением, аппаратура для передачи информации в инфракрасном диапазоне, по электросети и по телефонной линии.
18. Контактное и бесконтактное подключение к телефонной линии.
19. Телефонные коммутаторы.

20. Многоканальные станции сбора, архивирования, документирования и обработки речевых сообщений, которые используются для контроля стандартных абонентских телефонных линий.

21. Обычные, комбинированные и бесконтактные телефонные закладки.

22. Сканирующие радиоприемные устройства, камуфлированные радиоприемные устройства.

23. Антенны и антенные усилители.

24. Устройства панорамного обзора и анализа спектра сигналов.

25. Автоматизированные пункты радиоконтроля.

26. Компьютерные системы обработки перехваченных сигналов.

27. Средства контроля пейджинговых сообщений и сотовой связи.

28. Преодоление программных средств защиты, несанкционированное копирование информации, перехват информации в каналах связи, внедрение программных закладок и компьютерных вирусов, использование аппаратных закладок, перехват побочных электромагнитных излучений и наводок.

Критерии оценивания результатов экзамена: При выставлении баллов именно за экзамен (до 30 баллов в дополнение к баллам, полученным за другие виды отчетности) действует такой критерий оценки:

25-30 баллов

Студент дал полные, развернутые ответы на теоретический вопрос билета и правильно выполнил практическое задание, продемонстрировал знание функциональных возможностей, терминологии, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок.

17-24 баллов

Студент раскрыл в основном теоретический вопрос, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки, но все задание выполнено до конца.

10-16 баллов

При ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос. Студент сделал практическое задание лишь частично.

1-10 баллов

Ответ на теоретический вопрос свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Студент не смог ответить ни на один дополнительный вопрос. При этом студент не решил задачу или лишь частично (на ½ от задания).

Перевод оценки из 100-балльной в 4-балльную производится следующим образом:
- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов);
- хорошо – от 60 до 79 баллов;
- удовлетворительно – от 45 до 59 баллов;
- неудовлетворительно – менее 45 баллов.

Комплект контрольных работ

Для контроля освоения и/или расширения знаний, умений, владений предусмотрены несколько контрольных работ.

Модуль 1. Радиоэлектронная разведка

Письменная контрольная работа №1. Общие вопросы разведки

Вопросы

1. Криминалистическая характеристика преступлений, связанных с осуществлением технической радиоэлектронной разведки.
2. Правовая защита от компьютерных преступлений.
3. Особенности организационной и технической защиты информации, обрабатываемой средствами вычислительной техники.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	15
Выполнены пункты 1-3	25
Максимальный балл	25

Модуль 2. Радиоэлектронное подавление РЭС, скрытность и помехозащита РЭС

Письменная контрольная работа №2. Угрозы и уязвимости информационной безопасности

Вопросы

1. Сканирующие радиоприемные устройства, камуфлированные радиоприемные устройства.
2. Компьютерные системы обработки перехваченных сигналов.
3. Приборы ночного видения.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	15
Выполнены пункты 1-3	25
Максимальный балл	25

Комплект лабораторных работ

Для самостоятельного освоения и/или расширения знаний, умений, владений предусмотрены несколько лабораторных работ.

Модуль 1. Радиоэлектронная разведка

Типовая лабораторная работа №1. Модель угроз информационной безопасности

1. Выбрать объект защиты (документ, АРМ, ПК, помещение, АС и т.д.).

2. Собрать необходимую информацию.

3. Построить модель угроз информационной безопасности.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	10
Выполнены пункты 1-3	15
Максимальный балл	15

Типовая лабораторная работа 2. Модель нарушителя информационной безопасности

1. Выбрать объект защиты (документ, АРМ, ПК, помещение, АС и т.д.).

2. Собрать необходимую информацию.
3. Построить модель нарушителя безопасности.

Методические указания

а. Использовать известные уровни возможностей нарушителя, различные классификации нарушителя.

б. Помнить, для чего строится модель нарушителя.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	10
Выполнены пункты 1-3	15
Максимальный балл	15

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература:

1. Титов, А.А. Технические средства защиты информации : учебное пособие / А.А. Титов. -
Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. - 194 с.; То же [Электронный ресурс]. -
URL: http://biblioclub.ru/index.php?page=book&id=208661

2. Методы и средства инженерно-технической защиты информации : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. - 2-е изд., стер. - М. : Флинта,
2011. - 187 с. - (Организация и технология защиты информации). - ISBN 978-5-9765-1275-7 ;
То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93275

Дополнительная литература:

1. Креопалов В.В.. Технические средства и методы защиты информации: учебно-практическое пособие: учебное пособие [Электронный ресурс]/В.В. Креопалов.- М.: Евразийский открытый институт, 2011.-278с. -Режим доступа http://biblioclub.ru/book/90753/.

2. Березкин Е.Ф. Надежность и техническая диагностика систем: учебное пособие [Электронный ресурс]/Е.Ф. Березкин.- М.:МИФИ, 2012.-244с. -Режим доступа http://biblioclub.ru/book/231590/.

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
2. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
3. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
4. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;

5. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
6. www.newlibrary.ru – Новая электронная библиотека;
7. www. edu.ru – Федеральный портал российского образования;
8. www.elibrary.ru – Научная электронная библиотека;
9. www.nehudlit.ru – Электронная библиотека учебных материалов.
10. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
11. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
12. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специальных помещений и помещений для самостоятельной работы	***Вид занятий***	***Наименование оборудования, программного обеспечения***
1	**2**	**3**
Аудитория № 516	Лекции, семинары, практические занятия.	Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование.
Аудитория № 610	Лекции, семинары, практические занятия.	Учебная мебель, доска, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м.
Аудитория № 609	Лекции, семинары, практические занятия.	Учебная мебель, доска, мобильное мультимедийное оборудование.
Аудитория № 608	Лекции, семинары, практические занятия.	Учебная мебель, доска, мобильное мультимедийное оборудование
Аудитория № 613	Практические занятия, лабораторные работы.	Учебная мебель, доска, моноблок стационарный – 12 шт. с возможностью подключения к сети Интернет и доступа в электронную информационно-образовательную среду. Windows 8 Russian Windows Professional 8 Russian Upgrade. Договор №104 от 17.06.2013 г. Лицензии бессрочные. Microsoft Office Standard 2013 Russian. Договор №114

		от 12.11.2014 г. Лицензии бессрочные.

Приложение 1

МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Содержание рабочей программы
дисциплины «Техническая радиоэлектронная разведка»
на 7 семестр ОФО

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	55,2
лекций	16
практических/ семинарских	38
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	25,8
Учебных часов на самостоятельную работу обучающихся (СР)	20

Форма контроля:
экзамен 7 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / Сем	ЛР	СР		
1	2	3	4	5	6	7	8
1.	**Модуль 1. Радиоэлектронная разведка** **Раздел 1. Вводная часть:** 1.1. Содержание радиоэлектронной борьбы (РЭБ). Термины и определения. Основные составляющие РЭБ. 1.2. Задачи, решаемые средствами РЭБ. 1.3. Критерии и показатели эффективности работы радиоэлектронных систем и комплексов в условиях ведения РЭБ: информационные,	8	16	-	10	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Аудиторная работа, тесты

	энергетические, оперативно-тактические и военно-технические критерии. **Раздел 2. Радиоэлектронная разведка:** 2.1. Виды радиоэлектронных разведок. 2.2. Основные технические конфигурации средств систем и комплексов радиоэлектронной разведки. 2.3. Особенности обнаружения, определения параметров и воспроизведение сообщений средствами радиоэлектронных разведок. 2.4. Показатели эффективности систем и комплексов радиоэлектронных разведок. 2.5. Комплексы радиоэлектронных						

	разведок как системы массового обслуживания.						
2.	**Модуль 2. Радиоэлектронное подавление РЭС, скрытность и помехозащита РЭС Раздел 3. Радиоэлектронное подавление РЭС:** 3.1. Сущность радиоэлектронного подавления (РЭП). 3.2. Основные задачи, решаемые средствами РЭП. 3.3. Классификация средств РЭП. 3.4. Классификация помех радиоэлектронным системам, средствам и комплексам: пассивные и активные помехи; маскирующие,	8	16	-	10	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Аудиторная работа, тесты

	имитирующие, дезинформирующие помехи. 3.5. Особенности помеховых воздействий для РНС и СПИ. 3.6. Основные энергетические соотношения при создании активных помех РЭС. 3.7. Учет влияния взаимного пространственного положения подавляемого РЭС и помехопостановщика на энергетические соотношения. 3.8. Зоны эффективного действия постановщиков активных помех. 3.9. Эффективность РЭП систем навигации и связи при использовании различных заградительных помех. 3.10. Эффективность РЭП систем						

	навигации и связи при использовании имитационных помех. **Раздел 4. Скрытность и помехозащита РЭС:** 4.1. Скрытность объектов от средств радиоэлектронных разведок. 4.2. Скрытие РЭС как метод их защиты. 4.3. Основные методы скрытия объектов: снижение заметности в радиодиапазоне и создание помех средствам радиоэлектронного наблюдения. 4.4. Количественные показатели скрытности. 4.5. Энергетическая, структурная и информационная скрытность. 4.6. Скрытность широкополосных сигналов. 4.7. Понятие о помехозащищенности						

	как скрытности и помехоустойчивости. 4.8. Критерии оценки скрытности и помехоустойчивости. 4.9. Методы анализа помехоустойчивости систем и устройств радионавигации и радиосвязи.						
	Всего часов	16	32	-	20		