

МИНОБРНАУКИ РОССИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой  
ТО и ЗИ



А.А. Сирота

22.06.2022г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

Б1.О.41 Защита информации от утечки по техническим каналам

- 1. Шифр и наименование направления подготовки/специальности:**  
10.03.01 Информационная безопасность
- 2. Профиль подготовки/специализации:** безопасность компьютерных систем
- 3. Квалификация (степень) выпускника:** бакалавр
- 4. Форма образования:** очная
- 5. Кафедра, отвечающая за реализацию дисциплины:**  
Кафедра технологий обработки и защиты информации
- 6. Составители программы:**  
Нестеровский Олег Игоревич, к.т.н., доцент
- 7. Рекомендована:**  
Научно-методическим советом ФКН, протокол № 5 от 25.04.2022 г.

---

*(отметки о продлении вносятся вручную)*

---

---

---

---

**8. Учебный год:** 2024-2025

**Семестр(ы):** 6

## 9. Цели и задачи учебной дисциплины:

*Целями освоения учебной дисциплины являются:*

- изучение основ и принципов организации и технологии защиты информации (ЗИ) от утечки по техническим каналам с применением способов и средств ЗИ;
- изучение математических основ моделирования процессов защиты информации, получение профессиональных компетенций в области современных технологий защиты информации.

*Задачи учебной дисциплины:*

- обучение студентов базовым понятиям современных способов и средств ЗИ;
- обучение студентов базовым методам ЗИ;
- овладение практическими навыками применения способов и средств ЗИ;
- раскрытие физической сущности построения и эксплуатации информационных, информационно-измерительных и управляющих систем данных с точки зрения решения базовых задач обработки информации.

## 10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к блоку Б1 обязательных дисциплин общепрофессиональной части.

Входные знания в области физики, распространения сигналов, теории вероятностей и математической статистики, теории цифровой обработки сигналов, информатики.

## 11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.1	знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;	<b>знать:</b> сущность и понятия лицензирования в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации, характеристики их составляющих; <b>уметь:</b> классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; <b>владеть:</b> навыками определения основных характеристик при лицензировании в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств защиты информации
		ОПК-6.2	знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях;	<b>знать:</b> задачи органов защиты государственной тайны и служб защиты информации на предприятиях; <b>уметь:</b> определять основные пути решения задач органов защиты государственной тайны

				и служб защиты информации на предприятиях; <b>владеть:</b> основами решения задач органов защиты государственной тайны и служб защиты информации на предприятиях
		ОПК-6.3	знает систему организационных мер, направленных на защиту информации ограниченного доступа	<b>знать:</b> основные принципы организационных мер, направленных на защиту информации ограниченного доступа; <b>уметь:</b> анализировать возможные организационные меры, направленные на защиту информации ограниченного доступа; <b>владеть:</b> практическими навыками определения организационных мер, направленных на защиту информации ограниченного доступа
		ОПК-6.4	умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	<b>знать:</b> особенности формирования документов по защите информации ограниченного доступа в организации; <b>уметь:</b> применять знания об объекте при разработке документов по защите информации ограниченного доступа в организации; <b>владеть:</b> практическими навыками по разработке документов по защите информации ограниченного доступа в организации
		ОПК-6.5	умеет определить политику контроля доступа работников к информации ограниченного доступа	<b>знать:</b> особенности формирования документов по защите информации ограниченного доступа в организации; <b>уметь:</b> применять знания об объекте при разработке документов по защите информации ограниченного доступа в организации; <b>владеть:</b> практическими навыками по разработке документов по защите информации ограниченного доступа в организации
		ОПК-6.6	умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации	<b>знать:</b> основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; <b>уметь:</b> предъявлять требования к физической защите объекта и пропускному режиму в организации; <b>владеть:</b> практическими навыками по разработке требований, предъявляемых к физической защите объекта и пропускному режиму в организации
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач	ОПК-9.9	знает классификацию и количественные характеристики технических каналов утечки информации;	<b>знать:</b> основные принципы классификации и количественных характеристик технических каналов утечки информации; <b>уметь:</b> определять основные характеристики технических

профессиональной деятельности;			каналов утечки информации; <b>владеть:</b> практическими навыками классификации и определения количественных характеристик технических каналов утечки информации
	ОПК-9.10	знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;	<b>знать:</b> основные способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; <b>уметь:</b> определять необходимые способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; <b>владеть:</b> практическими навыками применения способов и средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации
	ОПК-9.11	знает организацию защиты информации от утечки по техническим каналам на объектах информатизации;	<b>знать:</b> основы принципов организации защиты информации от утечки по техническим каналам на объектах информатизации; <b>уметь:</b> определять необходимые принципы организации защиты информации от утечки по техническим каналам на объектах информатизации; <b>владеть:</b> практическими навыками организации защиты информации от утечки по техническим каналам на объектах информатизации
	ОПК-9.12	умеет пользоваться нормативными документами в области технической защиты информации;	<b>знать:</b> основные нормативные документы в области технической защиты информации; <b>уметь:</b> определить необходимые и пользоваться нормативными документами в области технической защиты информации; <b>владеть:</b> практическими навыками применения нормативных документов в области технической защиты информации
	ОПК-9.13	умеет анализировать и оценивать угрозы информационной безопасности объекта информатизации;	<b>знать:</b> угрозы информационной безопасности объекта информатизации; <b>уметь:</b> определить опасные угрозы информационной безопасности объекта информатизации; <b>владеть:</b> практическими навыками анализа и оценки угроз информационной безопасности объекта информатизации
	ОПК-9.14	владеет методами и средствами технической защиты информации.	<b>знать:</b> методы и средства технической защиты информации; <b>уметь:</b> определить необходимые методы и средства технической защиты информации;

				<b>владеть:</b> практическими навыками применения методов и средств технической защиты информации
--	--	--	--	---

**12. Объем дисциплины в зачетных единицах/час — 4/144.**

**Форма промежуточной аттестации: экзамен.**

**13. Трудоемкость по видам учебной работы**

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра 6	№ семестра	Итого
Аудиторные занятия		60	60		60
в том числе:	лекции	30	30		30
	практические	-	-		-
	лабораторные	30	30		30
Самостоятельная работа		48	48		48
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации (зачет – 0 час. / экзамен – ___ час.)		36	36		36
Итого:		144	144		144

**13.1. Содержание дисциплины**

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
<b>1. Лекции</b>			
1.1	Общие вопросы организации и обеспечения технической защиты информации	<ol style="list-style-type: none"> <li>1. Предметная область технической защиты информации.</li> <li>2. Исторические сведения и этапы развития технической защиты информации.</li> <li>3. Математические основы технической защиты информации</li> </ol>	
1.2	Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам	<ol style="list-style-type: none"> <li>4. Физические основы образования побочных электромагнитных излучений от ТСОИ, защита технических средств от утечки информации по этим каналам.</li> <li>5. Нормы эффективности защиты.</li> <li>6. Экранирование технических средств.</li> <li>7. Заземление технических средств.</li> <li>8. Развязывание информативных сигналов.</li> <li>9. Пространственное и линейное зашумление.</li> <li>10. Классификация и характеристики методов и средств поиска электронных устройств перехвата информации, их демаскирующие признаки.</li> <li>11. Методики измерения и расчета параметров информативных сигналов.</li> <li>12. Индикаторы электромагнитного поля, радиочастотомеры и интерсепторы.</li> <li>13. Сканерные приемники и анализаторы спектра.</li> <li>14. Программно-аппаратные и специальные комплексы контроля.</li> <li>15. Средства контроля проводных линий.</li> <li>16. Нелинейные локаторы, обнаружители пустот, металлоискатели и рентгеновские аппараты.</li> </ol>	

		<p>17. Методы поиска с использованием индикаторов электромагнитного поля, радиочастотометров и интерсепторов.</p> <p>18. Методы поиска с использованием сканерных приемников, анализаторов спектра, программно-аппаратных и специальных комплексов контроля.</p> <p>19. Методы контроля проводных линий.</p> <p>20. Методы поиска с использованием нелинейных локаторов, обнаружителей пустот, металлоискателей и рентгеновских аппаратов.</p> <p>21. Специальные проверки выделенных помещений</p>	
1.3	Организация ЗИ от утечки по техническим каналам	<p>22. Лицензирование деятельности и сертификация средств ЗИ.</p> <p>23. Аттестование объектов информатизации.</p> <p>24. Рекомендации по организации ЗИ от утечки по техническим каналам на объектах информатизации</p>	
<b>2. Практические занятия</b>			
2.1	нет		
<b>3. Лабораторные работы</b>			
3.1	Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам	<p>1. Экранирование технических средств. Заземление технических средств.</p> <p>2. Развязывание информативных сигналов. Пространственное и линейное зашумление.</p> <p>3. Методики измерения и расчета параметров информативных сигналов.</p> <p>4. Методы поиска с использованием сканерных приемников, анализаторов спектра, программно-аппаратных и специальных комплексов контроля.</p> <p>5. Методы контроля проводных линий.</p> <p>6. Методы поиска с использованием нелинейных локаторов, обнаружителей пустот, металлоискателей и рентгеновских аппаратов.</p>	

### 13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Сам. работа	Всего
1	Общие вопросы организации и обеспечения технической защиты информации	10	10	16	36
2	Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам	10	10	16	36
3	Организация ЗИ от утечки по техническим каналам	10	10	16	36
	Итого:	30	30	48	108

### 14. Методические указания для обучающихся по освоению дисциплины

1) При изучении дисциплины рекомендуется использовать следующие средства:

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;
- электронные версии учебников и методических указаний для выполнения лабораторно - практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на осно-

ве изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении лабораторных занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий защиты информации, излагаемых в рамках лекций.

4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций он-лайн и проведения лабораторно-практических занятий используются информационные ресурсы Образовательного портала "Электронный университет ВГУ (<https://edu.vsu.ru>), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

5) При использовании дистанционных образовательных технологий и электронного обучения обучающиеся должны выполнять все указания преподавателей, вовремя подключаться к онлайн - занятиям, ответственно подходить к заданиям для самостоятельной работы.

## 15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

### а) основная литература:

№ п/п	Источник
1	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : / Шаньгин В. Ф. — Москва : ДМК Пресс, 2010 .— 544 с. : ил., табл. ; 24 см .— (Администрирование и защита) .— ОГЛАВЛЕНИЕ кликните на URL-> .— Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника» .— Предм. указ.: с. 530-542 .— Библиогр.: с. 524-529 (105 назв.) .— ISBN 978-5-94074-518-1 .— <URL: <a href="http://e.lanbook.com/books/element.php?pl1_cid=25&amp;pl1_id=1122">http://e.lanbook.com/books/element.php?pl1_cid=25&amp;pl1_id=1122</a> >.

### б) дополнительная литература:

№ п/п	Источник
1	Астанин, Иван Константинович. Защита информации : учебное пособие для вузов / И.К. Астанин, Н.И. Астанин ; Воронеж. гос. ун-т, Лискинский филиал .— Воронеж : Воронеж. гос. ун-т, 2006 .— Библиогр. : с.169 .— ISBN 5-9273-1080-х.
2	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.
3	Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.

### в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)\*:

№ п/п	Ресурс
1	«Университетская библиотека online» - Контракт № 3010-06/05-20 от 28.12.2020, «Консультант студента» - Контракт № 3010-06/06-20 от 28.12.2020, ЭБС «Лань» - Договор №3010-06/03-21 от 10.03.2021, «РУКОНТ» (ИТС Контекстум) - Договор ДС-208 от 01.02.2018 ЭБС «Юрайт» - Договор № ДС-208 от 01.02.2021
2	Электронный каталог Научной библиотеки Воронежского государственного университета. – ( <a href="http://www.lib.vsu.ru/">http // www.lib.vsu.ru/</a> ).
3	Образовательный портал «Электронный университет ВГУ».– ( <a href="https://edu.vsu.ru/">https://edu.vsu.ru/</a> )

\* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

## **16. Перечень учебно-методического обеспечения для самостоятельной работы** *(учебно-методические рекомендации, пособия, задачки, методические указания по выполнению практических (контрольных) работ и др.)*

№ п/п	Источник
1	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков .— Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.

## **17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):**

Для реализации учебного процесса используются:

1) ПО Microsoft в рамках подписки "Imagine/Azure Dev Tools for Teaching", договор №3010-16/96-18 от 29 декабря 2018г.

2) ПО Матлаб в рамках подписки "Университетская лицензия на программный комплекс для ЭВМ - MathWorks, Headcount – 25 ": лицензия до 31.01.2022, сублицензионный контракт 3010-07/01-19 от 09.01.19.

3) LibreOffice v.5-7.

4) Foxit PDF Reader.

5) При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ (<https://edu.vsu.ru>), базирующегося на системе дистанционного обучения Moodle, развернутой в университете, а также другие доступные ресурсы сети Интернет.

## **18. Материально-техническое обеспечение дисциплины:**

*(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)*

1) Мультимедийная лекционная аудитория (корп.1а, ауд. № 380), ПК-Intel-G3420, рабочее место преподавателя: проектор, видеоконмутатор, специализированная мебель: доска меловая 1 шт., столы 31 шт., стулья 64 шт.; выход в Интернет, доступ к фондам учебно-методической документации и электронным изданиям.

2) Компьютерный класс (один из №1-4 корп. 1а, ауд. № 291, 293, 295, 387, 381), ПК-Intel-Core2/i3 14 шт., специализированная мебель: доска маркерная 1 шт., столы 14 шт., стулья 28 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.

3) Лаборатория технической защиты информации (корп. 1а, ауд. № 384а).

Состав лаборатории технической защиты информации: ST033P "Пиранья" - многофункциональный поисковый прибор, ST03.DA - дифференциальный низкочастотный усилитель, ST03.TEST - контрольное устройство; комплекс виброакустической защиты "Соната": Соната-ИПЗ, Соната-СА-65М, Соната-СВ-45М; генератор-виброизлучатель ( 5 октав) "ГШ-1000У"; генератор шума для защиты объектов вычислительной техники 1, 2 и 3 категорий от утечки информации; система автоматизированная оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок <Сигурд>.

## **19. Оценочные средства для проведения текущей и промежуточной аттестаций**

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:



№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Общие вопросы организации и обеспечения технической защиты информации	ОПК-6	ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-6.4 ОПК-6.5 ОПК-6.6	Письменная работа на проверку знаний понятия информации и информационной безопасности
2.	Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам	ОПК-9	ОПК-9.9 ОПК-9.10	Письменная работа на проверку знаний места и роли информационной безопасности в системе национальной безопасности Российской Федерации, основ государственной информационной политики
3.	Организация ЗИ от утечки по техническим каналам	ОПК-9	ОПК-9.11 ОПК-9.12 ОПК-9.13 ОПК-9.14	Письменная работа на проверку: знаний источников и классификации угроз информационной безопасности; умений классифицировать и оценивать угрозы информационной безопасности
Промежуточная аттестация форма контроля – Контрольная работа				

## 20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

### 20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью письменной работы на проверку знаний по разделам дисциплины (модулям).

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей аттестаций. На аттестации используется контрольно-измерительный материал, включающий в себя два-три вопроса.

Оценивание уровня сформированности компетенций осуществляется по содержанию вопросов, приведенных в таблице.

№	Содержание
1	Технический канал утечки информации, его характеристики
2	Пространственное электромагнитное зашумление. Особенности реализации
3	Мероприятия по защите информации и методы их реализации на режимных объектах
4	Технический контроль эффективности защиты информации. Основные задачи технического контроля и алгоритм его проведения
5	Средства защиты информации, сертифицируемые в системе сертификации по требованиям безопасности информации, и область их применения
6	Демаскирующие признаки электронных устройств перехвата информации
7	Причины и физические явления, обуславливающие возможные технические каналы утечки информации
8	Классификация методов и средств поиска электронных устройств перехвата информации
9	Технические каналы утечки информации, обрабатываемой техническими средствами
10	Назначение и принцип действия индикаторов электромагнитного поля. Особенности осуществления поиска электронных устройств перехвата информации с использованием индикаторов электромагнитного поля
11	Технические каналы утечки информации, акустической (речевой) информации
12	Назначение и принцип действия интерсепторов. Особенности осуществления поиска электронных устройств перехвата информации с использованием интерсепторов
13	Технические каналы утечки информации, передаваемой по каналам связи
14	Назначение и принцип действия радиочастотомеров. Особенности осуществления поиска электронных устройств перехвата информации с использованием радиочастотомеров
15	Экранирование технических средств. Виды, принципы и основные характеристики исполнения экранирования. Требования, предъявляемые к экранам

16	Назначение и принцип действия детекторов диктофонов. Особенности осуществления поиска электронных устройств перехвата информации с использованием детекторов диктофонов
17	Заземление технических средств. Схемы и принципы исполнения заземления. Основные требования, предъявляемые к системам заземления. Выражение для расчета сопротивления заземления
18	Назначение и принцип действия поискового прибора СРМ-700. Особенности осуществления поиска электронных устройств перехвата информации с использованием поискового прибора СРМ-700
19	Фильтрация информативных сигналов. Разделительные трансформаторы. Помехоподавляющие фильтры. Основные расчетные выражения, требования к защитным фильтрам
20	Назначение и принцип действия сканерных приемников. Особенности осуществления поиска электронных устройств перехвата информации с использованием сканерных приемников
21	Пространственное и линейное зашумление. Основные принципы реализации
22	Назначение и принцип действия анализаторов спектра. Особенности осуществления поиска электронных устройств перехвата информации с использованием анализаторов спектра

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании используется количественная шкала.

Критерии оценивания приведены таблице.

#### Критерии оценивания компетенций и шкала оценок

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

## 20.2. Промежуточная аттестация

Контроль успеваемости по дисциплине осуществляется с помощью контрольной работы на проверку знаний по дисциплине и собеседования по ее результатам.

Для оценивания результатов обучения на зачете с оценкой используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

- 1) знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;
- 2) умение проводить обоснование и представление основных теоретических

и практических результатов (теорем, алгоритмов, методик) с использованием математических выкладок, блок-схем, структурных схем и стандартных описаний к ним;

3) умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения лабораторно-практических заданий;

4) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;

5) владение навыками программирования и экспериментирования с компьютерными моделями алгоритмов обработки информации в среде Matlab в рамках выполняемых лабораторных заданий;

6) владение навыками проведения компьютерного эксперимента, тестирования компьютерных моделей алгоритмов обработки информации.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций):

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на зачете с оценкой используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

В ходе промежуточной аттестации используется контрольно-измерительный материал, включающий в себя два-три вопроса.

Оценивание уровня сформированности компетенций осуществляется по содержанию вопросов, приведенных в таблице.

№	Содержание
1	Технический канал утечки информации, его характеристики
2	Пространственное электромагнитное зашумление. Особенности реализации
3	Мероприятия по защите информации и методы их реализации на режимных объектах
4	Технический контроль эффективности защиты информации. Основные задачи технического контроля и алгоритм его проведения
5	Средства защиты информации, сертифицируемые в системе сертификации по требованиям безопасности информации, и область их применения
6	Демаскирующие признаки электронных устройств перехвата информации
7	Причины и физические явления, обуславливающие возможные технические каналы утечки информации
8	Классификация методов и средств поиска электронных устройств перехвата информации
9	Технические каналы утечки информации, обрабатываемой техническими средствами
10	Назначение и принцип действия индикаторов электромагнитного поля. Особенности осуществления поиска электронных устройств перехвата информации с использованием индикаторов электромагнитного поля
11	Технические каналы утечки информации, акустической (речевой) информации
12	Назначение и принцип действия интерсепторов. Особенности осуществления поиска электронных устройств перехвата информации с использованием интерсепторов
13	Технические каналы утечки информации, передаваемой по каналам связи
14	Назначение и принцип действия радиочастотомеров. Особенности осуществления поиска электронных устройств перехвата информации с использованием радиочастотомеров
15	Экранирование технических средств. Виды, принципы и основные характеристики исполнения экранирования. Требования, предъявляемые к экранам
16	Назначение и принцип действия детекторов диктофонов. Особенности осуществления поиска электронных устройств перехвата информации с использованием детекторов диктофонов
17	Заземление технических средств. Схемы и принципы исполнения заземления. Основные требования, предъявляемые к системам заземления. Выражение для расчета сопротивления заземления
18	Назначение и принцип действия поискового прибора СРМ-700. Особенности осуществления поиска электронных устройств перехвата информации с использованием поискового прибора СРМ-700

19	Фильтрация информативных сигналов. Разделительные трансформаторы. Помехоподавляющие фильтры. Основные расчетные выражения, требования к защитным фильтрам
20	Назначение и принцип действия сканерных приемников. Особенности осуществления поиска электронных устройств перехвата информации с использованием сканерных приемников
21	Пространственное и линейное зашумление. Основные принципы реализации
22	Назначение и принцип действия анализаторов спектра. Особенности осуществления поиска электронных устройств перехвата информации с использованием анализаторов спектра

Соотношение показателей, критериев и шкалы оценивания результатов обучения на зачете с оценкой представлено в следующей таблице.

#### **Критерии оценивания компетенций и шкала оценок**

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно