

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

«Утверждаю»  
Заведующий кафедрой ТО и ЗИ

«31» августа 2020 г.



А.А. Сирота

## РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.Б.49 Техническая защита информации

**1. Шифр и наименование направления подготовки/специальности:**  
10.05.01 Компьютерная безопасность

**2. Профиль подготовки/специализации:** для всех специализаций

**3. Квалификация (степень) выпускника:** специалист

**4. Форма образования:** очная

**5. Кафедра, отвечающая за реализацию дисциплины:**  
Кафедра технологий обработки и защиты информации

**6. Составители программы:**  
Гончаров Игорь Васильевич, к.т.н., доцент

**7. Рекомендована:**  
Научно-методическим советом ФКН, протокол № 7 от 31.08.2020 г.

---

*(отметки о продлении вносятся вручную)*

---

---

---

---

**8. Учебный год:** 2021-2022

**Семестр(ы):** 6

## 9. Цели и задачи учебной дисциплины:

Изучение основ и принципов организации и технологии защиты информации (ЗИ) от утечки по техническим каналам с применением способов и средств ЗИ в рамках комплексного обеспечения безопасности информационных систем и технологий, изучение математических основ моделирования процессов защиты информации, получение профессиональных компетенций в области современных технологий защиты информации.

Основные задачи 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 «Техническая защита информации» относится к блоку обязательных дисциплин обще-профессиональной 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 выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ОПК-9	Способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	<b>знать:</b> основные угрозы безопасности информации; <b>уметь:</b> применять основные правила и документы системы сертификации Российской Федерации; <b>владеть:</b> практическими навыками применения методов и средств обеспечения безопасности информации.
ПК-9	Способность участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы	<b>знать:</b> базовые понятия современных методов и технологий защиты информации; <b>уметь:</b> выявлять угрозы и технические каналы утечки информации; <b>владеть:</b> практическими навыками применения методов и средств технической защиты информации
ПК-12	Способность проводить инструментальный мониторинг защищенности компьютерных систем	<b>знать:</b> проблемы обеспечения безопасности информации, решаемые методами и средствами ЗИ от утечки по техническим каналам; <b>уметь:</b> описывать (моделировать) объекты защиты и угрозы безопасности информации; <b>владеть:</b> навыками контроля эффективности мер защиты с применением современных инструментальных средств
ПК-19	Способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации	<b>знать:</b> принципы и способы использования существующих средств ЗИ от утечки по техническим каналам; <b>уметь:</b> описывать (моделировать) объекты защиты и угрозы безопасности информации; <b>владеть:</b> навыками контроля эффективности мер защиты с применением современных инструментальных средств
ПК-20	Способность выполнять работы по восстановлению работоспособности средств	<b>знать:</b> принципы и способы использования существующих средств ЗИ от утечки по техническим каналам; <b>уметь:</b> применять наиболее эффективные методы и сред-

защиты информации при возникновении нештатных ситуаций	ства технической защиты информации; <b>владеть:</b> навыками контроля эффективности мер защиты с применением современных инструментальных средств
--	--

**12. Объем дисциплины в зачетных единицах/час — 3/108.**

**Форма промежуточной аттестации: экзамен.**

**13. Виды учебной работы:**

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		№ семестра 6	№ семестра	Итого
Аудиторные занятия	64	64		64
в том числе: лекции	32	32		32
практические	-	-		-
лабораторные	32	32		32
Самостоятельная работа	8	8		8
Форма промежуточной аттестации (зачет – 0 час. / экзамен – ___ час.)	36	36		36
Итого:	108	108		108

**13.1. Содержание дисциплины**

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
<b>1. Лекции</b>		
1.1	Общие вопросы организации и обеспечения технической защиты информации	1. Предметная область технической защиты информации. 2. Исторические сведения и этапы развития технической защиты информации. 3. Математические основы технической защиты информации
1.2	Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам	4. Физические основы образования побочных электромагнитных излучений от ТСОИ, защита технических средств от утечки информации по этим каналам. 5. Нормы эффективности защиты. 6. Экранирование технических средств. 7. Заземление технических средств. 8. Развязывание информативных сигналов. 9. Пространственное и линейное зашумление. 10. Классификация и характеристики методов и средств поиска электронных устройств перехвата информации, их демаскирующие признаки. 11. Методики измерения и расчета параметров информативных сигналов. 12. Индикаторы электромагнитного поля, радиочастотомеры и интерсепторы. 13. Сканерные приемники и анализаторы спектра. 14. Программно-аппаратные и специальные комплексы контроля. 15. Средства контроля проводных линий. 16. Нелинейные локаторы, обнаружители пустот, металлоискатели и рентгеновские аппараты. 17. Методы поиска с использованием индикаторов электромагнитного поля, радиочастотомеров и интерсепторов. 18. Методы поиска с использованием сканерных приемников, анализаторов спектра, программно-аппаратных и специальных комплексов контроля. 19. Методы контроля проводных линий. 20. Методы поиска с использованием нелинейных локаторов, обнаружителей пустот, металлоискателей и рентгеновских аппаратов. 21. Специальные проверки выделенных помещений
1.3	Организация ЗИ от утечки по техническим каналам	22. Лицензирование деятельности и сертификация средств ЗИ. 23. Аттестование объектов информатизации.

		24. Рекомендации по организации ЗИ от утечки по техническим каналам на объектах информатизации
<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	25. Экранирование технических средств. Заземление технических средств. 26. Развязывание информативных сигналов. Пространственное и линейное зашумление. 27. Методики измерения и расчета параметров информативных сигналов. 28. Методы поиска с использованием сканерных приемников, анализаторов спектра, программно-аппаратных и специальных комплексов контроля. 29. Методы контроля проводных линий. 30. Методы поиска с использованием нелинейных локаторов, обнаружителей пустот, металлоискателей и рентгеновских аппаратов.

### 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	-	20
2	Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам	10	10	4	24
3	Организация ЗИ от утечки по техническим каналам	12	12	4	28
	Итого:	32	32	8	72

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

*(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)*

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 основе 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 используется 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 клиньте 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
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.

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

№ п/п	Ресурс
3	Электронный каталог Научной библиотеки Воронежского государственного университета. – ( <a href="http://www.lib.vsu.ru/">http // www.lib.vsu.ru/</a> ).
4	Образовательный портал «Электронный университет ВГУ».– ( <a href="https://edu.vsu.ru/">https://edu.vsu.ru/</a> )
5	ЭБС «Издательства «Лань», Договор №3010-06/71-14 от 25.11.2014, ЭБС «Университетская библиотека online», Договор №3010-06/70-14 от 25.11.14, Национальный цифровой ресурс «РУКОНТ», Договор №ДС-208 от 01.02.2012
6	«Университетская библиотека online» - Контракт № 3010-07/33-19 от 11.11.2019 «Консультант студента» - Контракт № 3010-07/34-19 от 11.11.2019 ЭБС «Лань» - Договор 3010-04/05-20 от 26.02.2020 «РУКОНТ» (ИТС Контекстум) - Договор ДС-208 от 01.02.2018 ЭБС «Юрайт» - Договор № 43/8 от 10.02.2020

\* 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. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

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 MATLAB Classroom ver. 7.0, 10 конкурентных бессрочных лицензий на каждый, компоненты: Matlab, Simulink, Stateflow, 1 тулбокс, N 21127/VRN3 от 30.09.2011 (за счет проекта ЕК TEMPUS/ERAMIS).

3) 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.

4) 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. № 292), 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) 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»; измеритель звукового давления-виброметр (блок цифровой обработки БСП-МЗ, микрофон РСВ130Е20, ICP акселерометр AP98-100-01, Нетбук с ПО Тритон); оборудование создания тестового акустического сигнала (универсальная экранированная колонка УЭК-М2 с усилителем мощности усилитель мощности IPS-150 и генератором цифровым виброакустическим 2-х канальным SEL SP – 55); программно-аппаратный комплекс обнаружения и идентификации электронных устройств сотовой радиотелефонной связи и беспроводного доступа «САЛАМАНДРА 2»; анализатор спектра портативный Signal Hound USB-SA44B, из состава Парнас-ЭХО с антенной; Комплекс оценки эффективности защиты речевой информации от утечки по акустическим и акустоэлектрическим каналам «СМАРТ» на базе СКМ 21; Комплекс радиомониторинга «Кассандра».

## 19. Фонд оценочных средств:

### 19.1 Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции (или ее части)	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ОПК-9	<b>знать:</b> основные угрозы	Разделы 1-3	Контрольная работа

Способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	безопасности информации	Общие вопросы организации и обеспечения технической защиты информации. Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам. Организация ЗИ от утечки по техническим каналам.	по соответствующим разделам.
	<b>уметь:</b> применять основные правила и документы системы сертификации Российской Федерации	Разделы 1-3 Общие вопросы организации и обеспечения технической защиты информации. Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам. Организация ЗИ от утечки по техническим каналам.	Контрольная работа по соответствующим разделам. Лабораторные работы
	<b>владеть:</b> практическими навыками применения методов и средств обеспечения безопасности информации	Разделы 2-3 Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам. Организация ЗИ от утечки по техническим каналам.	Лабораторные работы
ПК-9 Способность участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы	<b>знать:</b> базовые понятия современных методов и технологий защиты информации	Разделы 1-3 Общие вопросы организации и обеспечения технической защиты информации. Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам. Организация ЗИ от утечки по техническим каналам.	Контрольная работа по соответствующим разделам.
	<b>уметь:</b> выявлять угрозы и технические каналы утечки информации	Разделы 1-3 Общие вопросы организации и обеспечения технической защиты информации. Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам. Организация ЗИ от утечки по техническим каналам.	Контрольная работа по соответствующим разделам. Лабораторные работы

	<b>владеть:</b> практическими навыками применения методов и средств технической защиты информации	Разделы 2-3 Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам. Организация ЗИ от утечки по техническим каналам.	Лабораторные работы
ПК-12 Способность проводить инструментальный мониторинг защищенности компьютерных систем	<b>знать:</b> проблемы обеспечения безопасности информации, решаемые методами и средствами ЗИ от утечки по техническим каналам	Разделы 2-3 Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам. Организация ЗИ от утечки по техническим каналам.	Контрольная работа по соответствующим разделам. Лабораторные работы
	<b>уметь:</b> описывать (моделировать) объекты защиты и угрозы безопасности информации	Разделы 2-3 Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам. Организация ЗИ от утечки по техническим каналам.	Контрольная работа по соответствующим разделам. Лабораторные работы
	<b>владеть:</b> навыками контроля эффективности мер защиты с применением современных инструментальных средств	Разделы 2-3 Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам. Организация ЗИ от утечки по техническим каналам.	Лабораторные работы
ПК-19 Способность производить проверки технического состояния и профилактические осмотры технических средств защиты информации	<b>знать:</b> принципы и способы использования существующих средств ЗИ от утечки по техническим каналам	Разделы 2-3 Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам. Организация ЗИ от утечки по техническим каналам.	Контрольная работа по соответствующим разделам.
	<b>уметь:</b> описывать (моделировать) объекты защиты и угрозы безопасности информации	Раздел 2 Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам	Контрольная работа по соответствующим разделам. Лабораторные работы
	<b>владеть:</b> навыками контроля эффективности мер защиты с применением современных инструментальных средств	Раздел 2 Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам	Лабораторные работы
ПК-20	<b>знать:</b> принципы постро-	Раздел 2	Контрольная работа



Способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	ения перспективных средств ЗИ от утечки по техническим каналам	Методы и средства ЗИ, обрабатываемой на объектах информатизации от утечки по техническим каналам	по соответствующим разделам. Лабораторные работы
	<b>уметь:</b> применять наиболее эффективные методы и средства технической защиты информации	Раздел 3 Организация ЗИ от утечки по техническим каналам	Контрольная работа по соответствующим разделам. Лабораторные работы
	<b>владеть:</b> навыками контроля эффективности мер защиты с применением современных инструментальных средств	Раздел 3 Организация ЗИ от утечки по техническим каналам	Контрольная работа по соответствующим разделам. Лабораторные работы
<b>Промежуточная аттестация</b>			Комплект КИМ

\* В графе «ФОС» в обязательном порядке перечисляются оценочные средства текущей и промежуточной аттестаций.

## 19.2. Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Для оценивания результатов обучения на экзамене 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) на государственном экзамене:

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

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

### Критерии оценивания компетенций и шкала оценок на экзамене

Критерии оценивания компетенций	Уровень	Шкала оценок
---------------------------------	---------	--------------

	сформированности компетенций	
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

### 19.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

#### 19.3.1 Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 19.2
3	Лабораторная работа	Содержит задания, предусматривающие разработку, тестирование и эксплуатацию моделей и алгоритмов анализа данных с использованием различных методов обучения.	При успешно выполнении работы ставится оценка зачтено и осуществляется допуск к экзамену, в противном случае ставится оценка не зачтено и обучающийся не допускается к экзамену.
4	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 заданий вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 19.2

#### 19.3.2. Примерный перечень вопросов к экзамену

№	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

### 19.3.3. Примеры заданий для выполнения лабораторных работ

#### Лабораторная работа № 2

##### «Исследование обеспечения защищенности информации с помощью многофункционального поискового прибора «Пиранья»»

###### Цель работы

Получение навыка проведения поисковых работ с помощью многофункционального прибора «Пиранья».

###### Форма контроля

Опрос в устной форме.

###### Количество отведённых аудиторных часов - 1

###### Содержание работы

Проверка работоспособности прибора во всех режимах работы, поиск и анализ сигналов.

###### Пример варианта задания:

1) Проверить работоспособность прибора во всех режимах работы, используя тестовое устройство в соответствии с руководством пользователя.

2) Исследовать амплитудно-частотный спектр телефонной линии прибором, при положенной трубке.

3) Исследовать амплитудно-частотный спектр телефонной линии прибором «Пиранья», при разговоре по телефону.

- 4) Проанализировать изменение составляющих спектра при подключении тех или иных приборов.
- 5) Исследовать амплитудно-частотный спектр электромагнитного поля в аудитории.
- 6) Исследовать амплитудно-частотный спектр инфракрасного поля в аудитории.
- 7) Предоставить устный отчет преподавателю о результатах работы.

**Примеры контрольных вопросов:**

- 1) Чем можно объяснить изменение амплитудно-частотного спектра электромагнитного поля при приближении к тем или иным предметам в аудитории?
- 2) Чем можно объяснить изменение амплитудно-частотного спектра инфракрасного поля при приближении к лампам освещения в аудитории?
- 3) Почему анализ информативных сигналов производится в спектре?
- 4) Какие сложности могут возникать при выполнении поисковых мероприятий?

**19.3.4. Пример контрольно-измерительного материала**

УТВЕРЖДАЮ  
Заведующий кафедрой технологий обработки и защиты информации

\_\_\_\_\_ А.А. Сирота  
\_\_\_.\_\_\_.2020

Направление подготовки / специальность 10.03.01 Компьютерная безопасность

Дисциплина Б1.Б.49 Техническая защита информации

Форма обучения Очное

Вид контроля Экзамен

Вид аттестации Промежуточная

**Контрольно-измерительный материал № 1**

1. Технический канал утечки информации, его характеристики
2. Пространственное электромагнитное зашумление. Особенности реализации

Преподаватель \_\_\_\_\_ И.В. Гончаров

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

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

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 могут использоваться количественные или качественные шкалы оценок.

**Промежуточная аттестация может включать в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и/или практическое**

**(ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.**

При оценивании используется количественная шкала. Критерии оценивания приведены выше в таблице раздела 19.2.