

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

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

Согласовано:
Председатель УМК института
Гильмутдинов /Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина

Инженерно-техническая защита информации(Б1.В.ДВ.02.01)

Часть, формируемая участниками образовательных отношений

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации
(в системе государственного и муниципального управления)

Квалификация
бакалавр

Разработчик (составитель)
к.б.н., доцент

Байрушин /Ф.Т. Байрушин/

Для приема: 2022 г.

Уфа 2022 г.

Составитель: Ф.Т. Байрушин

Рабочая программа дисциплины рассмотрена и одобрена 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	4
2	Цель и место дисциплины в структуре образовательной программы.....	5
3	Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)	5
4	Фонд оценочных средств по дисциплине	5
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.....	5
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	7
5	Учебно-методическое и информационное обеспечение дисциплины	17
5.1.	Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	17
5.2.	Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы	17
6	Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	17

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:

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
ПК-4- Способен проводить контроль защищенности информации	ИПК-2.1- знает методы контроля защищенности информации, каналы утечки информации, нормативно-правовую базу защиты информации	Знать: методы контроля защищенности информации, каналы утечки информации, нормативно-правовую базу защиты информации
	ИПК-2.2- умеет применять методы контроля защищенности информации, определять каналы утечки информации, применять нормативно-правовую базу защиты информации	Уметь: применять методы контроля защищенности информации, определять каналы утечки информации, применять нормативно-правовую базу защиты информации
	ИПК-2.3- владеет навыками применения методов контроля защищенности информации, определения каналов утечки информации, применения нормативно-правовой базы защиты информации	Владеть: навыками применения методов контроля защищенности информации, определения каналов утечки информации, применения нормативно-правовой базы защиты информации

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Инженерно-техническая защита информации» относится к части, обязательной для участников образовательных отношений.

Дисциплина изучается на 3 курсе, в 5,6 семестрах.

Цель изучения дисциплины: формирование у специалистов целостного представления о инженерно-технической защите информации.

Изучение дисциплины базируется на знаниях, умениях и навыках, сформированных в результате освоения студентами предшествующих дисциплин образовательной программы направления подготовки 10.03.01 «Средства вычислительной техники», «Основы электротехники и электроники», «Основы цифровой схемотехники».

Освоение дисциплины «Инженерно-техническая защита информации» служит основой для изучения таких дисциплин, как «Техническая радиоэлектронная разведка», «Основы комплексной защиты объектов информатизации», «Технические средства охраны», «Защита информации от утечки по техническим каналам». Полученные знания, навыки и умения используются в ходе выполнения выпускной квалификационной работы.

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

ПК-4- Способен проводить контроль защищенности информации

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ИПК-2.1- знает методы контроля защищенности информации, каналы утечки информации, нормативно-правовую базу защиты информации	Знать методы контроля защищенности информации, каналы утечки информации, нормативно-правовую базу защиты информации	Не знает методы контроля защищенности информации, каналы утечки информации, нормативно-правовую базу защиты информации	Знает методы контроля защищенности информации, каналы утечки информации, нормативно-правовую базу защиты информации
ИПК-2.2- умеет применять методы контроля защищенности информации, определять каналы утечки информации, применять нормативно-правовую базу защиты информации	Уметь применять методы контроля защищенности информации, определять каналы утечки информации, применять нормативно-правовую базу защиты информации	Не умеет применять методы контроля защищенности информации, определять каналы утечки информации, применять нормативно-правовую базу защиты информации	Умеет применять методы контроля защищенности информации, определять каналы утечки информации, применять нормативно-правовую базу защиты информации
ИПК-2.3- владеет навыками применения методов контроля защищенности информации,	Владеть навыками применения методов контроля защищенности информации, определения каналов утечки информации,	Не владеет навыками применения методов контроля защищенности информации, определения каналов	Владеет навыками применения методов контроля защищенности информации, определения каналов утечки информации, применения

определения каналов утечки информации, применения нормативно-правовой базы защиты информации	применения нормативно-правовой базы защиты информации	утечки информации, применения нормативно-правовой базы защиты информации	нормативно-правовой базы защиты информации
--	---	--	--

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ИПК-2.1- знает методы контроля защищенности информации, каналы утечки информации, нормативно-правовую базу защиты информации	Знать методы контроля защищенности информации, каналы утечки информации, нормативно-правовую базу защиты информации	Имеет фрагментарные представления о методах контроля защищенности информации, каналах утечки информации, нормативно-правовой базе защиты информации	В целом знает о методах контроля защищенности информации, каналах утечки информации, нормативно-правовой базе защиты информации	Знает о методах контроля защищенности информации, каналах утечки информации, нормативно-правовой базе защиты информации, допускает незначительные ошибки	Демонстрирует целостные знания о методах контроля защищенности информации, каналах утечки информации, нормативно-правовой базе защиты информации
ИПК-2.2- умеет применять методы контроля защищенности информации, определять каналы утечки информации, применять нормативно-правовую базу защиты информации	Уметь применять методы контроля защищенности информации, определять каналы утечки информации, применять нормативно-правовую базу защиты информации	Не умеет применять методы контроля защищенности информации, определять каналы утечки информации, применять нормативно-правовую базу защиты информации	В целом умеет применять методы контроля защищенности информации	Умеет применять методы контроля защищенности информации, определять каналы утечки информации, применять нормативно-правовую базу защиты информации, допускает незначительные ошибки	Умеет применять защищенности информации, определять каналы утечки информации, применять нормативно-правовую базу защиты информации
ИПК-2.3- владеет	Владеть навыками	Не способен овладеть	В целом способен	Способен овладеть	Способен овладеть

навыками применения методов контроля защищенности информации, определения каналов утечки информации, применения нормативно-правовой базы защиты информации	применения методов контроля защищенности информации, определения каналов утечки информации, применения нормативно-правовой базы защиты информации	навыками применения методов контроля защищенности информации, определения каналов утечки информации, применения нормативно-правовой базы защиты информации	овладеть навыками применения методов контроля защищенности информации	навыками применения методов контроля защищенности информации, определения каналов утечки информации, применения нормативно-правовой базы защиты информации, допускает незначительные ошибки	навыками применения методов контроля защищенности информации, определения каналов утечки информации, применения нормативно-правовой базы защиты информации
--	---	--	---	---	--

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
ИПК-2.1- знать методы управления защитой информации в автоматизированных системах, каналы утечки информации, нормативно-правовую базу защиты информации	Знает: методы управления защитой информации в автоматизированных системах, каналы утечки информации, нормативно-правовую базу защиты информации	Устный индивидуальный / групповой опрос, тестирование
ИПК-2.2- умеет применять методы управления защитой информации в автоматизированных системах, определять каналы утечки информации, применять нормативно-правовую базу защиты информации	Умеет: применять методы управления защитой информации в автоматизированных системах, определять каналы утечки информации, применять нормативно-правовую базу защиты информации	Устный индивидуальный / групповой опрос, тестирование
ИПК-2.3- владеет навыками применения методов управления защитой информации в автоматизированных системах, определения каналов утечки информации, применения нормативно-правовой базы защиты информации	Владеет: навыками применения методов управления защитой информации в автоматизированных системах, определения каналов утечки информации, применения нормативно-правовой базы защиты информации	Устный индивидуальный / групповой опрос, тестирование

--	--	--

Критериями оценивания при *модульно-рейтинговой системе* являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), 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».

Рейтинг – план дисциплины Инженерно-техническая защита информации

Направление подготовки 10.03.01 Информационная безопасность

Курс 3 семестр 5

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль			0	25
1. Аудиторная работа	1	5	0	5
2. Домашние задания	1	5	0	5
3. Практические работы	3	5	0	15
Рубежный контроль				5
1. Тестовые задания	0,2	25	0	5
Всего			0	30
Модуль 2				
Текущий контроль			0	25
1. Аудиторная работа	1	5	0	5
2. Домашние задания	1	5	0	5
3. Практические работы	3	5	0	15
Рубежный контроль				5
1. Тестовые задания	0,2	25	0	5
Всего			0	30
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных				-6

занятий				
2. Посещение практических занятий				-10
Итоговый контроль				
зачет			0	40

Рейтинг – план дисциплины
Инженерно-техническая защита информации

Направление подготовки 10.03.01 Информационная безопасность

Курс 3 семестр 6

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 3				
Текущий контроль			0	25
1. Аудиторная работа	1	5	0	5
2. Домашние задания	1	5	0	5
3. Практические работы	3	5	0	15
Рубежный контроль				5
1. Тестовые задания	0,2	25	0	5
Всего			0	30
Модуль 4				
Текущий контроль			0	25
1. Аудиторная работа	1	5	0	5
2. Домашние задания	1	5	0	5
3. Практические работы	3	5	0	15
Рубежный контроль				5
1. Тестовые задания	0,2	25	0	5
Всего			0	30
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
3. Посещение лекционных занятий				-6
4. Посещение практических занятий				-10
Итоговый контроль				
экзамен			0	30

Оценочные средства

Типовые зачетные материалы

Зачет состоит из двух вопросов, отражающих соответственно материал первого и второго модуля.

Вопросы для проведения зачета

1. Системный подход как основа создания эффективной инженерно-технической защиты информации
2. Использование физических эффектов в технических системах
3. Закономерности проявления физических эффектов
4. Закономерности технической реализации физических эффектов
5. Особенности построения физических схем
6. Базы данных по физическим эффектам
7. Классификация технических каналов утечки информации. Роль физических эффектов в образовании каналов утечки информации.
8. Классификация акустических каналов утечки информации
9. Прямой акустический канал
10. Акустовибрационный канал
11. Акустоэлектрический канал утечки информации
12. Акусторадиоэлектронный канал
13. Акустопараметрический канал
14. Акустооптический канал
15. Классификация электрических каналов утечки информации
16. Канал утечки информации по телефонной линии
17. Канал утечки информации по цепям электропитания
18. Канал утечки информации по цепям заземления
19. Классификация оптических каналов утечки информации
20. Системы обнаружения оптических устройств. Средства противодействия утечке информации по оптическим каналам.
21. Классификация электромагнитных каналов утечки информации
22. Методы и средства предотвращения утечки информации по радиотехническим каналам
23. Методы и средства контроля утечки информации по радиоканалам
24. Источники электромагнитных излучений и наводок
25. Использование эффектов: паразитных связей, электромагнитных наводок, с целью образования случайных антенн
26. Методы пассивной защиты информации от утечки через ПЭМИН
27. Методы активной защиты информации от утечки через ПЭМИН
28. Методы средства и контроля побочных электромагнитных излучений и наводок
29. Передача информации с помощью лазера
30. Структурные схемы образования комплексных каналов утечки информации

Критерии оценки при проведении зачета

Критерии оценки	Распределение баллов
<ul style="list-style-type: none">• Ответы на поставленные вопросы излагаются логично, последовательно и не требуют дополнительных пояснений.• Полно раскрываются причинно-следственные связи между явлениями и событиями.• Делаются обоснованные выводы.• Демонстрируются глубокие знания базовых нормативно-правовых актов.• Соблюдаются нормы литературной речи.	зачтено
<ul style="list-style-type: none">• Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине.• Не раскрываются причинно-следственные связи между явлениями и событиями.• Не проводится анализ.• Выводы отсутствуют.• Ответы на дополнительные вопросы отсутствуют.• Имеются заметные нарушения норм литературной речи.	Не зачтено

Экзамен

Структура экзаменационного билета:

Экзаменационный билет состоит из двух вопросов, отражающих соответственно материал первого, второго, модуля

Типовые экзаменационные материалы

1. Угрозы безопасности информации и меры по их предотвращению.
2. Видовые демаскирующие признаки объектов в видимом и инфракрасном диапазонах света.
3. Демаскирующие признаки аналоговых сигналов
4. Типовая структура технического канала утечки информации.
5. Концепция и методы технической защиты информации
6. Понятие экранирования. Основные положения
7. Контроль защищенности информации на объекте ВТ от утечки по каналу ПЭМИ.
8. Демаскирующие признаки дискретных сигналов
9. Технический контроль акустической защищенности выделенного помещения.
10. Материально-вещественный канал утечки информации. Способы восстановления информации на магнитных носителях.
11. Аттестация объектов информатизации. Мероприятия по выявлению и оценке свойств каналов утечки .
12. Технический контроль акустической защищенности выделенного помещения.
13. Контроль технических средств и систем .
14. Принципы построения системы ИТЗИ: равнопрочность рубежей, непрерывность, подконтрольность и гибкость системы защиты
15. Утечка информации по цепям электропитания
16. Технический контроль акустической защищенности выделенного помещения.
17. Акустический и виброакустический контроль

18. Низкочастотные и высокочастотные излучения технических средств
19. Виды технических каналов утечки информации
20. Оптические каналы утечки информации
21. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам.
22. Анализаторы линий и устройства контроля проводных линий
23. Демаскирующие признаки дискретных сигналов .
24. Электромагнитные излучения распределенных источников.
25. Виды технических каналов утечки информации
26. Оптические каналы утечки информации
27. Принципы построения системы ИТЗИ: равнопрочность рубежей, непрерывность, подконтрольность и гибкость системы защиты
28. Утечка информации по цепям электропитания
29. Технический контроль акустической защищенности выделенного помещения.
30. Аттестация объектов информатизации
31. Концепция и методы инженерно-технической защиты информации
32. Понятие экранирования. Основные положения
33. Демаскирующие признаки аналоговых сигналов
34. Типовая структура технического канала утечки информации.
35. Принципы построения системы ИТЗИ: многозональность и многорубежность
36. Способы защиты информации с помощью технологии Proximity и смарт-карт
37. Технические каналы утечки информации. Структура и классификация.
38. Электромагнитный канал утечки информации .
39. Методы выявления закладных устройств.
40. Пассивные методы защиты речевой информации от её утечки через ограждающие конструкции. Рекомендации по выбору ограждающих конструкций.
41. Активные методы и средства защиты речевой информации от утечки по техническим каналам, Характеристика генераторов шума.
42. Методы и средства защиты информации в телефонных линиях связи.

Пример экзаменационного билета:

Форма 1.4.-33

МИНОБРНАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Направление подготовки 10.03.01 Информационная безопасность

Дисциплина Инженерно-техническая защита информации

- 1 Угрозы безопасности информации и меры по их предотвращению.
- 2 Видовые демаскирующие признаки объектов в видимом и инфракрасном диапазонах света.

Зав. кафедрой УИБ

А.С. Исмагилова

Критерии оценивания результатов экзамена для ОФО:

Критерии оценки (в баллах):

- 25-30 баллов выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок;

- 17-24 баллов выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки;

- 10-16 баллов выставляется студенту, если 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 основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос. Студент не решил задачу или при решении допущены грубые ошибки;

- 1-10 баллов выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос. Устанавливается следующая градация перевода оценки из многобалльной в четырех балльную:

Типовые тестовые задания

При изучении дисциплины используются тестовые задания закрытого типа. Каждое тестовое задание включает вопрос и 4 варианта ответов к нему. Тестирование выполняется в письменной или электронной форме.

Необходимо выбрать один ответ из предложенных вариантов.

1. Компьютер — это:

- а) устройство для работы с текстами;
- б) электронное вычислительное устройство для обработки чисел;
- в) устройство для хранения информации любого вида;
- г) многофункциональное электронное устройство для работы с информацией;
- д) устройство для обработки аналоговых сигналов.
- е) другое

2. Постоянное запоминающее устройство служит для:

- а) хранения программ начальной загрузки компьютера и тестирования его узлов;
- б) хранения программы пользователя во время работы;
- в) записи особо ценных прикладных программ;
- г) хранения постоянно используемых программ;

- д) постоянного хранения особо ценных документов.
- е) другое

3. Процесс хранения информации на внешних носителях принципиально отличается от процесса хранения информации в оперативной памяти:

а) тем, что на внешних носителях информация может храниться после отключения питания компьютера;

- б) объемом хранимой информации;
- в) различной скоростью доступа к хранимой информации;
- г) возможностью защиты информации;
- д) способами доступа к хранимой информации.
- е) другое

4. Манипулятор “мышь” — это устройство:

- а) модуляции и демодуляции;
- б) считывания информации;
- в) долговременного хранения информации;
- г) ввода информации;
- д) для подключения принтера к компьютеру.
- е) другое

5. С использованием команды MD в MS DOS создается:

- а) текстовый файл;
- б) командный файл;
- в) пустой каталог;
- г) совокупность каталогов;
- д) файл IO.SYS.
- е) другое

6. Одной из основных характеристик компьютера является быстродействие, которое характеризуется:

- а) количеством операций в секунду;
- б) количеством выполняемых одновременно программ;
- в) временем организации связи между АЛУ и ОЗУ;
- г) количеством вводимых символов;
- д) количеством подключенных устройств;
- е) другое

7. Имя и тип файла разделяются между собой:

- а) символом “ . ”;
- б) символом “ - ”;
- в) пробелом
- г) символом “*”
- д) символом « _ »
- е) другое

8. Скорость работы компьютера зависит от:

- а) тактовой частоты обработки информации в процессоре;
- б) наличия или отсутствия подключенного принтера;
- в) организации интерфейса операционной системы;
- г) объема внешнего запоминающего устройства;
- д) объема обрабатываемой информации.

е) другое

9 Во время исполнения прикладная программа хранится:

- а) в видеопамяти;
- б) в процессоре;
- в) в оперативной памяти;
- г) на жестком диске;
- д) в ПЗУ.
- е) другое

10 Для подключения компьютера к телефонной сети используется:

- а) модем;
- б) факс;
- в) сканер;
- г) принтер;
- д) монитор.
- е) другое

11 Расширение имени файла, как правило, характеризует:

- а) время создания файла;
- б) объем файла;
- в) место, занимаемое файлом на диске;
- г) тип информации, содержащейся в файле;
- д) место создания файла.
- е) другое

12 Команда COPY предназначена для копирования в MS DOS:

- а) файлов и каталогов;
- б) только текстовых файлов;
- в) только каталогов;
- г) только командных файлов;
- д) утилит MSDOS.
- е) другое

13 . Максимальная длина двоичного кода, который может обрабатываться или передаваться процессором целиком:

- а) Кэш;
- б) BIOS;
- в) Разрядность;
- г) Тактовая частота
- д) Контроллер;
- е) другое

14 . В какой из последовательностей единицы измерения информации указаны в порядке возрастания:

- а) байт, килобайт, мегабайт, бит;
- б) килобайт, байт, бит, мегабайт;
- в) байт, мегабайт, килобайт, гигабайт;
- г) мегабайт, килобайт, гигабайт, байт;
- д) байт, килобайт, мегабайт, гигабайт. е) другое.

15 . Винчестер предназначен для:

- а) подключения периферийных узлов к магистрали;
- б) управления работой ЭВМ по заданной программе;
- в) хранения информации;

16 Память, используемая для хранения больших объемов информации:

- а) оперативная память;
- б) гибкий магнитный диск;
- в) постоянная память (ПЗУ);

17 Микропроцессор имеет в своем составе:

- а) устройство ввода;
- б) внутренние регистры;
- в) арифметико-логическое устройство;

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста (25 вопросов в варианте)	Неправильный ответ / Правильный ответ	0/0,2 за один ответ Всего: 5 баллов

Устный индивидуальный опрос

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

Студент излагает содержание вопроса изученной темы.

Критерии и методика оценивания:

- 5 баллов выставляется студенту, если точно используется специализированная терминология, показано уверенное владение нормативной базой;
- 4 балла выставляется студенту, допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология;
- 3 балла выставляется студенту, 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 студенту, если точно используется специализированная терминология, показано уверенное владение нормативной базой;
- 4 балла выставляется студенту, допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология;
- 3 балла выставляется студенту, нет общего понимания вопроса, имеются затруднения или допущены ошибки в определении понятий, использовании терминологии.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература:

1. Корниенко, В. Т. Обеспечение безопасности передачи информации в радиотехнических системах с примерами в проектах LabVIEW : учебное пособие : [16+] / В. Т. Корниенко. – Москва ; Берлин : Директ-Медиа, 2020. – 81 с. : ил., табл., схем. – URL: <https://biblioclub.ru/index.php?page=book&id=597410>
2. Голиков А. М. Защита информации от утечки по техническим каналам: учебное пособие[Электронный ресурс]Томский государственный университет систем управления и радиоэлектроники, 2015. –256с.Режим доступа http://http://biblioclub.ru/index.php?page=book_red&id=480636&sr=1
3. Иванов, А. В. Оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок : учебное пособие : [16+] / А. В. Иванов. – Новосибирск : Новосибирский государственный технический университет, 2018. – 64 с. : URL: <https://biblioclub.ru/index.php?page=book&id=575420> (
4. Рябов Б. А. , Малахов С. М. , Хотунцев Ю. Л. Практикум по радиоэлектронике Москва: МПГУ, 2017.- 108 стр. Режимдоступа https://biblioclub.ru/index.php?page=book_red&id=471195&sr=1
- 5.Гульятеева, Т. А. Основы защиты информации : учебное пособие : [16+] / Т. А. Гульятеева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=574730>

Дополнительная литература

1. Голиков А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие[Электронный ресурс]Томский государственный университет систем управления и радиоэлектроники, 2015. –256с.Режим доступа http://http://biblioclub.ru/index.php?page=book_red&id=480636&sr=1
2. Сердюк В. А. Организация и технологии защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие[Электронный ресурс] Москва: Издательский дом Высшей школы экономики, 2015 .- 574с. -Режим доступа http://biblioclub.ru/index.php?page=book_red&id=440285&sr=1

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/catalog/>
4. Электронный учебный курс «Теория организации» <http://sdo.bashedu.ru/course/view.php?id=127>
5. Справочная правовая система «Гарант» – <http://www.garant.ru>.
6. Справочная правовая система «КонсультантПлюс» – <http://www.consultant-plus.ru>.

6. Материально-техническая база, необходимая для осуществления

образовательного процесса по дисциплине

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	2	3
<p>1. учебная аудитория для проведения занятий лекционного типа: аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус).</p> <p>2. учебная аудитория для проведения лабораторных работ: Лаборатория полигон технической защиты информации № 508 (гуманитарный корпус), компьютерный класс, аудитория 404 (гуманитарный корпус), аудитория 420 (гуманитарный корпус).</p> <p>3. учебная аудитория для проведения групповых и индивидуальных консультаций, учебная аудитория для текущего контроля и промежуточной аттестации: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 510 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус).</p>	<p align="center">Аудитория № 403</p> <p>Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия.</p> <p align="center">Аудитория № 405</p> <p>Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96*244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей, ActivPanel 21S – 1 шт., Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт., Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт., Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96*244*244MV (XT1000E) -1 шт.</p> <p align="center">Аудитория № 413</p> <p>Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p align="center">Аудитория № 415</p> <p>Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p align="center">Аудитория № 416</p> <p>Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт.</p> <p align="center">Аудитория № 418</p> <p>Учебная мебель, доска, Экран настенный Lumien Master Piktura 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт.</p>	<p>1. Права на программы для ЭВМ операционная система для персонального компьютера Win SL 8 Russian OLP NL AcademicEdition Legalization GetGenuine. Права на программы для ЭВМ обновление операционной системы для персонального компьютера Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.</p> <p>2. Программа для ЭВМ Office Standard 2013 Russian OLP NL AcademicEdition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.</p> <p>3. Права на использование программного обеспечения антивирус для рабочих станций, файловых серверов, серверов масштаба предприятия, мобильных устройств Kaspersky Endpoint Security для бизнеса - Стандартный, подписка на 1 год. Договор №31705437224 от 04.09.2017 г.</p> <p>4. Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ». Модуль «Программный комплекс поиска текстовых заимствований в открытых источниках сети интернет «Антиплагиат-интернет». Договор №229 от 02.05.2017 г.</p> <p>5. Справочная правовая система Консультант Плюс. Договор №31705775411 от 07.12.2017 г.</p>

<p>(гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).</p> <p>4. учебная аудитория для курсового проектирования (выполнения курсовых работ): аудитория №613 (гуманитарный корпус).</p> <p>5. учебная аудитория для проведения занятий семинарского типа: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 510 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус).</p> <p>6. помещения для самостоятельной работы: читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус).</p> <p>7.помещение для хранения и профилактического обслуживания учебного оборудования: аудитория № 523 (гуманитарный корпус).</p>	<p>Аудитория № 419 Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт.</p> <p>Аудитория № 515 Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром.</p> <p>Аудитория № 516 Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.</p> <p>Аудитория № 509 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 510 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 608 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 609 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 610 Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м.</p> <p>Аудитория № 613 Учебная мебель, доска, моноблок стационарный – 15 шт.</p> <p>Компьютерный класс аудитория № 420 Учебная мебель, моноблоки стационарные 15 шт.</p> <p>Компьютерный класс аудитория № 404 Учебная мебель, компьютеры -15 штук.</p> <p>Аудитория 402 читальный зал библиотеки Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура,</p>	
---	---	--

	<p>мышь, стеллажи, шкафы картотечные, комбинированные.</p> <p>Лаборатория полигон технической защиты информации № 508</p> <p>Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технической защиты информации, комплекс мониторинга WiFi сетей "Зодиак II", универсальный ком-плект инструментов для проведения работ по специальным провер-кам и специальным обследованиям Калейдоскоп-П2, многофункциональный поисковый прибор ST-031M "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон".</p> <p>Аудитория № 523</p> <p>Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.</p>	
--	---	--

Приложение 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины «Инженерно-техническая защита информации» на 5,6 семестр

очная форма обучения

Рабочую программу осуществляют:

Лекции: к.б.н., доцент Байрушин Ф.Т.

Практические занятия: к.б.н., доцент Байрушин Ф.Т.

Вид работы	Объем дисциплины	
	5 семестр	6 семестр
Общая трудоемкость дисциплины (ЗЕТ / часов)	2 ЗЕТ / 72 часа	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	54,2	49,2
лекций	18	16
практических/ семинарских	36	32
лабораторных	-	-
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2	1,2
из них, предусмотренные на выполнение курсовой работы / курсового проекта	0	0
Учебных часов на самостоятельную работу обучающихся (СР)	17,8	31,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	0	0
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	0	27

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / Сем	ЛАБ	СР		
1	2	3	4		6	8	9
1.	Модуль 1. 1. Основные направления инженерно-технической защиты	1	2		2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
2.	2. Основные свойства информации как предмета защиты. Виды защищаемой информации	1	2		3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
3.	3. Источники и носители информации	2	4		3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы,	Устный индивидуальный / групповой опрос, тестирование
4.	Модуль 2 1. Угрозы безопасности информации Виды угроз безопасности информации	2	4		2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
5.	2. Принципы добывания информации и технология добывания информации	1	2		3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
6.	3 Технические каналы утечки информации	2	4		2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование

7.	4. Оптические каналы утечки информации	2	4		2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
8.	5 Радиоэлектронные каналы утечки информации	2	4		2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
9	6. Акустические каналы утечки информации	2	4		2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
	Модуль 3					Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
10	1.Комплексное использование каналов утечки информации	2	4		2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
11	2.Основные методы защиты информации техническими средствами	1	2		3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
12	3.Способы и средства противодействия наблюдению в оптическом диапазоне	1	2		3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
13	4.Способы и средства противодействия радиолокационному . и гидроакустическому наблюдению	2	4		2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
14	5.Способы и средства информационного скрывтия речевой информации от подслушивания	2	4		2	Самостоятельное изучение рекомендуемой основной и	Устный индивидуальный / групповой опрос, тестирование

						дополнительной литературы	
15	6.Способы и средства предотвращения несанкционированной записи речевой информации на диктофон	2	4		2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
	Модуль 4					Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
16	1.Принципы контроля телефонных линий и цепей электропитания.	1	2		3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
17	2.Технические средства подавления сигналов закладных устройств.	2	4		2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
18	3.Способы и средства контроля помещений на отсутствие закладных устройств	2	4		3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
19	4.Способы и средства предотвращения утечки информации через побочные излучения и наводки	2	4		3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
20	5.Способы подавления опасных электрических сигналов акустоэлектрических преобразователей	2	4		3,6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование
21	Всего часов	34	68		49.6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный индивидуальный / групповой опрос, тестирование

