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

Утверждено:
на заседании кафедры
протокол № 8 от « 24 » февраля 2021 г.
Зав. кафедрой _____ /Исмагилова А.С.

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина
Защита информации в системах связи

Часть, формируемая участниками образовательных отношений (Б1.В.ДВ.04.02)

программа специалитета

Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация
«Организация и технологии защиты информации (по отраслям)»

Квалификация
специалист по защите информации

Разработчик (составитель) к.ф.-м.н., старший преподаватель кафедры управления информационной безопасностью	/ Юнусова Д.С.

Для приема: 2021 г.

Уфа 2021 г.

Составитель: Юнусова Дарья Сергеевна

Рабочая программа дисциплины *утверждена* на заседании кафедры протокол от «_24_» _февраля_____ 2021 г. № _8_

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

Заведующий кафедрой / Исмагилова А.С. /

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

Заведующий кафедрой _____/ Исмагилова А.С. /

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

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций (при наличии ОПК)	**Формируемая компетенция (с указанием кода)**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения по дисциплине**
Аналитическая	ПК-3. Способен анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации	ИПК-3.1 Знает основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Знать основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации
		ИПК-3.2 Умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации	Уметь анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации
		ИПК-3.3 Владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Владеть использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации
Проектно-технологическая	ПК-4. Способен определять основные угрозы безопасности информации в автоматизированных системах	ИПК-4.1 Знает принципы и методы определения основные угроз безопасности информации в автоматизированных системах	Знать принципы и методы определения основные угроз безопасности информации в автоматизированных системах
		ИПК-4.2 Умеет определять основные угрозы безопасности информации в	Уметь определять основные угрозы безопасности информации в

		автоматизированных системах	автоматизированных системах
		ИПК-4.3 Владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах	Владеть принципами и методами определения основные угроз безопасности информации в автоматизированных системах
Организационно-управленческая	ПК-1. Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей	ИПК-1.1 Знает современные технологии построения безопасных информационных систем	Знать современные технологии построения безопасных информационных систем
		ИПК-1.2 Умеет анализировать и оценивать угрозы информационной безопасности	Уметь анализировать и оценивать угрозы информационной безопасности
		ИПК-1.3 Владеет методами формирования требований по защите информации	Владеть методами формирования требований по защите информации

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Защита информации в системах связи» относится к части, формируемой участниками образовательных отношений.

Дисциплина изучается на 5 курсе в семестрах 9 и А.

Целью изучения дисциплины «Защита информации в системах связи» является формирование у студентов целостного представления об общих закономерностях развития и функционирования систем защиты информации.

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

Содержание рабочей программы представлено в Приложении № 1.

4. Фонд оценочных средств по дисциплине

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

ПК-3. Способен анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
ИПК-3.1 Знает основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Знать основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Не знает основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Знает основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации
ИПК-3.2 Умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации	Уметь анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации	Не умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации	Умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации
ИПК-3.3 Владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Владеть использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Не владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации

ПК-4. Способен определять основные угрозы безопасности информации в автоматизированных системах

Код и наименование индикатора достижения	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»

компетенции			
ИПК-4.1 Знает принципы и методы определения основные угроз безопасности информации в автоматизированных системах	Знать принципы и методы определения основные угроз безопасности информации в автоматизированных системах	Не знает принципы и методы определения основные угроз безопасности информации в автоматизированных системах	Знает принципы и методы определения основные угроз безопасности информации в автоматизированных системах
ИПК-4.2 Умеет определять основные угрозы безопасности информации в автоматизированных системах	Уметь определять основные угрозы безопасности информации в автоматизированных системах	Не умеет определять основные угрозы безопасности информации в автоматизированных системах	Умеет определять основные угрозы безопасности информации в автоматизированных системах
ИПК-4.3 Владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах	Владеть принципами и методами определения основные угроз безопасности информации в автоматизированных системах	Не владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах	Владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах

ПК-1. Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
ИПК-1.1 Знает современные технологии построения безопасных информационных систем	Знать современные технологии построения безопасных информационных систем	Не знает современные технологии построения безопасных информационных систем	Знает современные технологии построения безопасных информационных систем
ИПК-1.2 Умеет анализировать и оценивать угрозы информационной безопасности	Уметь анализировать и оценивать угрозы информационной безопасности	Не умеет анализировать и оценивать угрозы информационной безопасности	Умеет анализировать и оценивать угрозы информационной безопасности
ИПК-1.3 Владеет методами формирования требований по защите информации	Владеть методами формирования требований по защите информации	Не владеет методами формирования требований по защите информации	Владеет методами формирования требований по защите информации

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для зачета: текущий контроль –

максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов).

ПК-3. Способен анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств 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-3.1 Знает основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Знать основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Не знает основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Имеет фрагментарные знания об основных принципах и методах анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	В целом знает основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Знает основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации
ИПК-3.2 Умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации	Уметь анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации	Не умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств	Умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффектив	В целом умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и	Умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффектив

		защиты информации	ности применяемых средств защиты информации, но допускает значительные ошибки	эффективности применяемых средств защиты информации, но допускает незначительные ошибки	ности применяемых средств защиты информации
ИПК-3.3 Владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Владеть использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Не владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации, но допускает значительные ошибки	Уверенно владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации, но допускает незначительные ошибки	Владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации

ПК-4. Способен определять основные угрозы безопасности информации в автоматизированных системах

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Неудовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)

ИПК-4.1 Знает принципы и методы определения основные угроз безопасности информации в автоматизированных системах	Знать принципы и методы определения основные угроз безопасности информации в автоматизированных системах	Не знает принципы и методы определения основные угроз безопасности информации в автоматизированных системах	Имеет фрагментарные знания о принципах и методах определения основных угроз безопасности информации в автоматизированных системах	В целом знает принципы и методы определения основные угроз безопасности информации в автоматизированных системах	Знает принципы и методы определения основные угроз безопасности информации в автоматизированных системах
ИПК-4.2 Умеет определять основные угрозы безопасности информации в автоматизированных системах	Уметь определять основные угрозы безопасности информации в автоматизированных системах	Не умеет определять основные угрозы безопасности информации в автоматизированных системах	Умеет определять основные угрозы безопасности информации в автоматизированных системах, но допускает значительные ошибки	В целом умеет определять основные угрозы безопасности информации в автоматизированных системах, но допускает незначительные ошибки	Умеет определять основные угрозы безопасности информации в автоматизированных системах
ИПК-4.3 Владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах	Владеть принципами и методами определения основные угроз безопасности информации в автоматизированных системах	Не владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах	Владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах, но допускает	Уверенно владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах, но допускае	Владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах

			значительные ошибки	т незначительные ошибки	

ПК-1. Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ИПК-1.1 Знает современные технологии построения безопасных информационных систем	Знать современные технологии построения безопасных информационных систем	Не знает современные технологии построения безопасных информационных систем	Имеет фрагментарные знания о современных технологиях построения безопасных информационных систем	В целом знает современные технологии построения безопасных информационных систем	Знает современные технологии построения безопасных информационных систем
ИПК-1.2 Умеет анализировать и оценивать угрозы информационной безопасности	Уметь анализировать и оценивать угрозы информационной безопасности	Не умеет анализировать и оценивать угрозы информационной безопасности	Умеет анализировать и оценивать угрозы информационной безопасности, но допускает значительные ошибки	В целом умеет анализировать и оценивать угрозы информационной безопасности, но допускает незначительные ошибки	Умеет анализировать и оценивать угрозы информационной безопасности
ИПК-1.3 Владеет методами формирования требований по защите информации	Владеть методами формирования требований по защите информации	Не владеет методами формирования требований по защите информации	Владеет методами формирования требований по защите информации, но допускает значительные ошибки	Уверенно владеет методами формирования требований по защите информации, но допускает незначительные	Владеет методами формирования требований по защите информации

				ошибки	

Критериями оценивания 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:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

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

ПК-3. Способен анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ИПК-3.1 Знает основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Знать основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	тестирование, практическое задание
ИПК-3.2 Умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации	Уметь анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации	тестирование, практическое задание
ИПК-3.3 Владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	Владеть использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	тестирование, практическое задание

ПК-4. Способен определять основные угрозы безопасности информации в автоматизированных системах

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ИПК-4.1 Знает принципы и методы определения основные угроз безопасности информации в автоматизированных системах	Знать принципы и методы определения основные угроз безопасности информации в автоматизированных системах	тестирование, практическое задание
ИПК-4.2 Умеет определять основные угрозы безопасности информации в автоматизированных системах	Уметь определять основные угрозы безопасности информации в автоматизированных системах	тестирование, практическое задание
ИПК-4.3 Владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах	Владеть принципами и методами определения основные угроз безопасности информации в автоматизированных системах	тестирование, практическое задание

ПК-1. Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ИПК-1.1 Знает современные технологии построения безопасных информационных систем	Знать современные технологии построения безопасных информационных систем	тестирование, практическое задание
ИПК-1.2 Умеет анализировать и оценивать угрозы информационной безопасности	Уметь анализировать и оценивать угрозы информационной безопасности	тестирование, практическое задание
ИПК-1.1 Знает современные технологии построения безопасных информационных систем	Знать современные технологии построения безопасных информационных систем	тестирование, практическое задание

Рейтинг – план дисциплины
«Защита информации в системах связи»

Специальность: 10.05.05 Безопасность информационных технологий в правоохранительной сфере

курс 5, семестр 9

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Основные понятия и положения защиты информации в системах связи				
Текущий контроль				
Практическая работа	5	5	0	25
Рубежный контроль				
Тест	25	1	0	25
Всего			0	50
Модуль 2. Общие принципы защиты информации в системах связи				
Текущий контроль				
Практическая работа	5	5	0	25
Рубежный контроль				
Тест	25	1	0	25
Всего			0	50
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего			0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10
Итоговый контроль				
1.Зачет				

Рейтинг – план дисциплины
«Защита информации в системах связи»

Специальность: 10.05.05 Безопасность информационных технологий в правоохранительной сфере

курс 5, семестр А

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Методы и средства защиты информации в системах связи				
Текущий контроль				
Практическая работа	5	4	0	20
Рубежный контроль				
Тест	15	1	0	15
Всего			0	35
Модуль 2. Защита информации в каналах общего пользования				
Текущий контроль				
Практическая работа	5	4	0	20

Рубежный контроль				
Тест	15	1	0	15
Всего			0	35
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего			0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10
Итоговый контроль				
1.Экзамен	30	1	0	30

Вопросы к зачету

1. Демаскирующие признаки сигналов.
2. Запись и съем информации с носителей.
3. Опасные сигналы и их источники.
4. Побочные преобразования акустических сигналов в электрические.
5. Паразитные связи и наводки.
6. Низкочастотные и высокочастотные излучения технических средств.
7. Электромагнитные излучения распределенных источников.
8. Сигналы и шумы. Спектры сигналов.
9. Демаскирующие признаки сигналов.
10. Запись и съем информации с носителя.
11. Опасные сигналы и их источники.
12. Побочные преобразования акустических сигналов в электрические сигналы.
13. Паразитные связи и наводки.
14. Надежность канала связи. Помехоустойчивость каналов связи.
15. Трафик. Скорость передачи информации в канале связи.
16. Требования к качественным характеристикам систем связи.
17. Утечка информации по цепям электропитания.
18. Утечка информации по цепям заземления.
19. Типовая структура и виды технических каналов утечки информации.
20. Основные показатели технических каналов утечки информации.
21. Комплексное использование технических каналов утечки информации.
22. Акустические каналы утечки информации.
23. Оптические каналы утечки информации.
24. Виды радиоэлектронных каналов утечки информации.
25. Распространение опасных электрических и радиосигналов в радиоэлектронном канале утечки информации.
26. Структура системы инженерно-технической защиты информации.
27. Подсистема физической защиты источников информации.
28. Структура подкомплекса технических средств охраны.
29. Структура подкомплекса нейтрализации угроз.
30. Подсистема инженерно-технической защиты информации от ее утечки.
31. Правовое обеспечение информационной безопасности систем связи в РФ.

32. Основные законодательные акты, регулирующие отношения, связанные с правовой защитой и использованием интеллектуальной собственности в области информационных сетей и систем.

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов).

Экзамен

Структура экзаменационного билета

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

Примерные вопросы для экзамена

1. Демаскирующие признаки сигналов.
2. Запись и съем информации с носителей.
3. Опасные сигналы и их источники.
4. Побочные преобразования акустических сигналов в электрические.
5. Паразитные связи и наводки.
6. Низкочастотные и высокочастотные излучения технических средств.
7. Электромагнитные излучения распределенных источников.
8. Сигналы и шумы. Спектры сигналов.
9. Демаскирующие признаки сигналов.
10. Запись и съем информации с носителя.
11. Опасные сигналы и их источники.
12. Побочные преобразования акустических сигналов в электрические сигналы.
13. Паразитные связи и наводки.
14. Надежность канала связи. Помехоустойчивость каналов связи.
15. Трафик. Скорость передачи информации в канале связи.
16. Требования к качественным характеристикам систем связи.
17. Утечка информации по цепям электропитания.
18. Утечка информации по цепям заземления.
19. Типовая структура и виды технических каналов утечки информации.
20. Основные показатели технических каналов утечки информации.
21. Комплексное использование технических каналов утечки информации.
22. Акустические каналы утечки информации.
23. Оптические каналы утечки информации.
24. Виды радиоэлектронных каналов утечки информации.
25. Распространение опасных электрических и радиосигналов в радиоэлектронном канале утечки информации.
26. Структура системы инженерно-технической защиты информации.
27. Подсистема физической защиты источников информации.
28. Структура подкомплекса технических средств охраны.
29. Структура подкомплекса нейтрализации угроз.
30. Подсистема инженерно-технической защиты информации от ее утечки.

31. Правовое обеспечение информационной безопасности систем связи в РФ.
32. Основные законодательные акты, регулирующие отношения, связанные с правовой защитой и использованием интеллектуальной собственности в области информационных сетей и систем.
33. Утечка информации по системам электропитания и заземления.
34. Технические каналы утечки информации.
35. Акустические каналы утечки информации.
36. Оптические каналы утечки информации.
37. Радиоэлектронные каналы утечки информации.
38. Методы и средства защиты информации от ее утечки по техническим каналам.
39. Возможные угрозы абоненту телефонной линии связи
40. Устройства контроля телефонных линий.
41. Способы и аппаратура защиты телефонных линий
42. Пассивные и активные способы защиты телефонных линий.
43. Изменение уровня напряжения в телефонной линии как способ защиты от подслушивания.
44. Криптографическая защита телефонных сообщений.
45. Архитектура GSM-сети. Особенности работы.
46. Защита информации в каналах сотовой связи. Атаки, использующие уязвимости базовых мобильных технологий.
47. Защита информации в каналах сотовой связи. Атаки, использующие уязвимости технологии SMS.
48. Атаки, использующие уязвимости технологии Bluetooth.
49. Защита информации в каналах сотовой связи. Атаки, использующие использующие уязвимости мобильных Интернет-технологий.
50. IP-телефония. Сценарии организации, протоколы, алгоритмы обработки и передачи речи.
51. IP-телефония. Функции основных компонентов сети IP-телефонии на основе H.323.
52. IP-телефония. Протоколы, используемые при передачи речи по IP-сети.
53. SIP. Компоненты сети IP-телефонии на основе SIP.
54. Возможные угрозы IP-телефонии (перехват данных, отказ в облуживании, подмена номера, кража сервисов, неожидаемые вызовы, несанкционированное изменение конфигурации, мошенничество со счетом).
55. Обеспечение безопасности IP телефонии. Стандарты IP-телефонии и механизмы их безопасности. Шифрование, обеспечение конфиденциальности.
56. Режимы применения ESP и AH. Протоколы IKE.
57. Оборудование для построения сетей (кабели, концентратор, коммутатор, маршрутизатор, мост, повторитель).
58. Виды серверов и их предназначение.
59. Настройка простейшей сети.
60. Рабочие группы и общие ресурсы.
61. Критерии оценки безопасности систем связи
62. Общие положения по эксплуатации систем связей
63. Особенности эксплуатации и администрирования защищенных систем связей

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 терминологии, основных понятий, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы.

- 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.

- 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.

- 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 четырехбалльную:

Экзамены:

- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов),
- хорошо – от 60 до 79 баллов,
- удовлетворительно – от 45 до 59 баллов,
- неудовлетворительно – менее 45 баллов.

Пример экзаменационного билета:

Форма 1.4.-33

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ
КАФЕДРА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Дисциплина Защита информации в системах связи

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Запись и съем информации с носителей.
2. Атаки, использующие уязвимости технологии Bluetooth.

Зав. Кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

Примерная тематика курсовых проектов (работ)

Курсовое проектирование не предусмотрено

Типовые тестовые задания

При изучении дисциплины используются тестовые задания закрытого типа. Каждое тестовое задание включает вопрос и варианты ответов к нему. Тестирование выполняется в письменной форме.
Необходимо выбрать один ответ из предложенных вариантов.

Тест № 1

Модуль 1. Основные понятия и положения защиты информации в системах связи

Вопрос №1

Совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства:

а) угроза информационной безопасности;

б) предполагаемые действия иностранных государств;

в) деятельность иностранных разведок.

Вопрос №2

Не являются видами угроз информационной безопасности:

а) внутренние угрозы;

б) внешние угрозы;

в) значительные угрозы.

Вопрос №3

Не являются видами угроз информационной безопасности:

а) угрозы военные;

б) угрозы потенциальные;

в) угрозы реальные.

Тест № 2

Модуль 2. Общие принципы защиты информации в системах связи

Вопрос №1

К принципам обеспечения безопасности относится:

а) согласованность;

б) взаимная ответственность личности, общества и государства;

в) децентрализации и демократизм.

Вопрос №2

Защита информации в современных системах ее обработки это:

а) обеспечение доступности информации для пользователей;

б) обеспечение целостности информации при ее передаче, обработке и хранении;

в) обеспечение конфиденциальности информации.

Вопрос №3

Для реализации принципа разграничения потоков информации необходимо, чтобы:

а) информация, предназначенная разным пользователям, передавалась в разных потоках;

б) информация разного уровня конфиденциальности передавалась в разных потоках;

в) информация с ограниченным доступом передавалась по выделенным линиям связи.

Тест № 3

Модуль 3. Методы и средства защиты информации в системах связи

Вопрос №1

К методам обеспечения информационной безопасности Российской Федерации относятся:

а) правовые;

б) неправовые;

в) легальные.

Вопрос №2

К методам обеспечения информационной безопасности Российской Федерации относятся:

а) методы принуждения;

б) организационно-технические;

в) секретные.

Вопрос №3

К методам обеспечения информационной безопасности Российской Федерации относятся:

а) оперативные;

б) конструктивные;

в) экономические.

Тест № 4

Модуль 4. Защита информации в каналах общего пользования

Вопрос №1

Сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации это:

а) сфера хранения информации;

б) информационная сфера;

в) сфера государственного регулирования информации.

Вопрос №2

Какие из перечисленных мер составляют комплексную стратегию предотвращения вирусного подавления?

а) запрет доступа (препятствие проникновению вирусных программ в систему);

б) обнаружение (обнаружение присутствия в системе вирусной программы);

в) сдерживание (изоляция пораженной части системы от непораженной);

г) ликвидация (уничтожение вирусов до того, как они произведут свое разрушительное действие);

д) восстановление нормального функционирования (восстановление разрушенных файлов с использованием резервных файлов);

е) альтернативные меры (меры, не допускающие вывода системы из строя даже в случае поражения особо сложными и оригинальными вирусными программами).

Вопрос №3

Какие из перечисленных факторов приводят к возрастанию уязвимости современных автоматизированных систем для компьютерных вирусов?

а) расширение применения распределенной цифровой обработки информации;

б) использование перепрограммируемых встроенный ЭВМ и сетей связи;

в) стандартизация ЭВМ, программного обеспечения, форматов сообщений, каналов и процедур передачи данных.

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста (25 вопросов в варианте)	Неправильный ответ / Правильный ответ	
Модуль 1		1
Модуль 2		1
Модуль 3		0,6
Модуль 4		0,6

Комплект практических заданий

Для самостоятельного освоения и/или расширения знаний, умений, владений предусмотрены несколько практических занятий, к которым студенты должны подготовить доклады по темам практических занятий.

Модуль 1. Основные понятия и положения защиты информации в системах связи

Темы практических заданий

1. Общие критерии безопасности информации.
2. Особенности защиты информации в системах связи.
3. Криптография.
4. Стеганография.
5. Защита компьютерных сетей

Критерии оценивания

Практическое занятие оценивается в 5 баллов. Основными критериями при оценке практических занятий являются соответствие содержания доклада освещаемому вопросу, полнота раскрываемой в докладе темы, структура доклада и подача информации, а также правильные, аргументированные ответы на вопросы по докладу и степень участия в дискуссии.

5 баллов студент получает, если вопрос доклада освещен в полном объеме и изложен грамотным языком в правильной логической последовательности с точным использованием специализированной терминологии; если при этом показано уверенное владение материалом; студент правильно и аргументировано ответил на все вопросы по докладу и активно принимал участие в дискуссии.

4 балла студент получает, если вопрос доклада освещен в полном объеме, но имеются некоторые недостатки. К примеру, в работе допущены один-два недочета при освещении основного содержания ответа и/или нет определенной логической последовательности, неточно используется специализированная терминология или подача материала трудна для восприятия.

3 балла студент получает, если он не полно осветил вопрос, либо если доклад не структурирован, а также если студент не смог аргументировано ответить на вопросы по теме доклада.

2 балл студент получает, если он осветил вопрос неполно, не смог правильно ответить на вопросы по теме доклада.

1 балл студент получает, если содержание доклада соответствует теме освещаемого вопроса, но студент не показал общее понимание вопроса, не смог ответить на вопросы по теме доклада.

0 баллов студент получает при несоответствии содержания доклада освещаемому вопросу.

Модуль 2. Общие принципы защиты информации в системах связи

Темы практических заданий

1. Сигналы и шумы в системах связи
2. Скорость передачи связи в канале связи
3. Помехоустойчивость каналов связи с гауссовскими шумами
4. Радиотехнические характеристики телекоммуникационных радиоканалов

Критерии оценивания

Практическое занятие оценивается в 5 баллов. Основными критериями при оценке практических занятий являются соответствие содержания доклада освещаемому вопросу, полнота раскрываемой в докладе темы, структура доклада и подача информации, а также правильные, аргументированные ответы на вопросы по докладу и степень участия в дискуссии.

5 баллов студент получает, если вопрос доклада освещен в полном объеме и изложен грамотным языком в правильной логической последовательности с точным использованием

специализированной терминологии; если при этом показано уверенное владение материалом; студент правильно и аргументировано ответил на все вопросы по докладу и активно принимал участие в дискуссии.

4 балла студент получает, если вопрос доклада освещен в полном объеме, но имеются некоторые недостатки. К примеру, в работе допущены один-два недочета при освещении основного содержания ответа и/или нет определенной логической последовательности, неточно используется специализированная терминология или подача материала трудна для восприятия.

3 балла студент получает, если он не полно осветил вопрос, либо если доклад не структурирован, а также если студент не смог аргументировано ответить на вопросы по теме доклада.

2 балл студент получает, если он осветил вопрос неполно, не смог правильно ответить на вопросы по теме доклада.

1 балл студент получает, если содержание доклада соответствует теме освещаемого вопроса, но студент не показал общее понимание вопроса, не смог ответить на вопросы по теме доклада.

0 баллов студент получает при несоответствии содержания доклада освещаемому вопросу.

Модуль 3. Методы и средства защиты информации в системах связи

Темы практических заданий

1. Законодательная база в области защиты информации.
2. Структура государственных органов обеспечивающих защиту информации.
3. Общая характеристика организационных методов ЗИ.
4. Действующие стандарты РФ по защите информации.
5. Понятие политики безопасности.
6. Уязвимости. Модели основных политик от НСД.

Критерии оценивания

Практическое занятие оценивается в 5 баллов. Основными критериями при оценке практических занятий являются соответствие содержания доклада освещаемому вопросу, полнота раскрываемой в докладе темы, структура доклада и подача информации, а также правильные, аргументированные ответы на вопросы по докладу и степень участия в дискуссии.

5 баллов студент получает, если вопрос доклада освещен в полном объеме и изложен грамотным языком в правильной логической последовательности с точным использованием специализированной терминологии; если при этом показано уверенное владение материалом; студент правильно и аргументировано ответил на все вопросы по докладу и активно принимал участие в дискуссии.

4 балла студент получает, если вопрос доклада освещен в полном объеме, но имеются некоторые недостатки. К примеру, в работе допущены один-два недочета при освещении основного содержания ответа и/или нет определенной логической последовательности, неточно используется специализированная терминология или подача материала трудна для восприятия.

3 балла студент получает, если он не полно осветил вопрос, либо если доклад не структурирован, а также если студент не смог аргументировано ответить на вопросы по теме доклада.

2 балл студент получает, если он осветил вопрос неполно, не смог правильно ответить на вопросы по теме доклада.

1 балл студент получает, если содержание доклада соответствует теме освещаемого вопроса, но студент не показал общее понимание вопроса, не смог ответить на вопросы по теме доклада.

0 баллов студент получает при несоответствии содержания доклада освещаемому вопросу.

Модуль 4. Защита информации в каналах общего пользования

Темы практических заданий

1. Современные принципы построения абонентского оборудования в телефонных линиях связи
2. Угрозы и защита информации в телефонных каналах
3. Современные конструкции систем защищенной мобильной связи
4. Современные конструкции систем защищенной IP-телефонии

Критерии оценивания

Практическое занятие оценивается в 5 баллов. Основными критериями при оценке практических занятий являются соответствие содержания доклада освещаемому вопросу, полнота раскрываемой в докладе темы, структура доклада и подача информации, а также правильные, аргументированные ответы на вопросы по докладу и степень участия в дискуссии.

5 баллов студент получает, если вопрос доклада освещен в полном объеме и изложен грамотным языком в правильной логической последовательности с точным использованием специализированной терминологии; если при этом показано уверенное владение материалом; студент правильно и аргументировано ответил на все вопросы по докладу и активно принимал участие в дискуссии.

4 балла студент получает, если вопрос доклада освещен в полном объеме, но имеются некоторые недостатки. К примеру, в работе допущены один-два недочета при освещении основного содержания ответа и/или нет определенной логической последовательности, неточно используется специализированная терминология или подача материала трудна для восприятия.

3 балла студент получает, если он не полно осветил вопрос, либо если доклад не структурирован, а также если студент не смог аргументировано ответить на вопросы по теме доклада.

2 балл студент получает, если он осветил вопрос неполно, не смог правильно ответить на вопросы по теме доклада.

1 балл студент получает, если содержание доклада соответствует теме освещаемого вопроса, но студент не показал общее понимание вопроса, не смог ответить на вопросы по теме доклада.

0 баллов студент получает при несоответствии содержания доклада освещаемому вопросу.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. Аверченков, В. И. Служба защиты информации: организация и управление : [16+] / В. И. Аверченков, М. Ю. Рытов. – 3-е изд., стер. – Москва : ФЛИНТА, 2016. – 186 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93356

2. Гультяева, Т. А. Основы защиты информации : учебное пособие : [16+] / Т. А. Гультяева. – 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

3. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - Москва : Горячая линия-Телеком, 2015. - 585 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0424-8 ; То же [Электронный ресурс]. -

URL: http://biblioclub.ru/index.php?page=book&id=457143
4. Малюк, А.А. Защита информации в информационном обществе : учебное пособие / А.А. Малюк. - Москва : Горячая линия-Телеком, 2015. - 229 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0481-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457170
5. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности : учебное пособие / Ю.И. Коваленко. - Москва: Горячая линия - Телеком, 2012. - 140 с. : ил. - Библиогр. в кн. - ISBN 978-5-9912-0261-9 ; То же [Электронный ресурс]. -
URL: http://biblioclub.ru/index.php?page=book&id=253538

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

1. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
2. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
3. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
4. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
5. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
6. www.newlibrary.ru – Новая электронная библиотека;
7. www. edu.ru – Федеральный портал российского образования;
8. www.elibrary.ru – Научная электронная библиотека;
9. www.nehudlit.ru – Электронная библиотека учебных материалов.
10. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
11. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
12. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

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

Наименование специальных помещений и помещений для самостоятельной работы	Вид занятий	Оснащенность специальных помещений и помещений для самостоятельной работы
1	2	3
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). **2.** ***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 № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **3.** ***учебная аудитория для курсового проектирования (выполнения курсовых работ):*** аудитория № 613 (гуманитарный корпус). **4.** ***учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418	Лекции, практические занятия, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKG WMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром Promethean ActivBoard 387 RPO MOUNT EST -1 шт., Ком-ер встраиваемый в кафедру INTEL Core i3-4150/DDr3 4 Gb/HDD, Экран настенный Draper Luma AV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H – 1 шт. , Мультимедиа-проектор Panasonic PT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKG WMS45 – 1 шт. , Терминал видео конференц-связи LifeSize Icon 600 Camera 10x Phone 2nd Generation – 1 шт., Экран настенный Draper Luma AV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ MA1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ MA1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean

(гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). ***5. 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 № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **6. *помещения для самостоятельной работы:*** аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).		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. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **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. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Аудитория 402 читальный зал библиотеки** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.

Приложение № 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Защита информации в системах связи** на 9 семестр
___очная_ф/о___

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	54,2
лекций	18
практических/ семинарских	36
лабораторных	
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на самостоятельную работу обучающихся (СР)	53,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на подготовку к зачету (Контроль)	–

Форма контроля
Зачет 9 семестр

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Защита информации в системах связи** на А семестр
очная ф/о

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	49,2
лекций	16
практических/ семинарских	32
лабораторных	
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на самостоятельную работу обучающихся (СР)	49,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на подготовку к зачету (Контроль)	45

Форма контроля
Экзамен А семестр

Семестр 9

№	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	ЛР	СРС		
1	2	3	4	5	6	8	9
Модуль 1. Основные понятия и положения защиты информации в системах связи							
1	Введение в дисциплину	2	4		6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
2	Угрозы безопасности информации	2	4		7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
3	Злоумышленники угроз	2	4		7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
4	Основные понятия и положения защиты информации в системах связи	4	6		7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
Модуль 2. Общие принципы защиты информации в системах связи							
5	Качественные характеристики каналов связи	2	4		7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы,	Практическая работа, тестирование

						интернет-источников.	
6	Требования к качественным характеристикам систем связи	2	6		7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
7	Утечка информации	2	4		6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
8	Основы организационно-правового обеспечения информационной безопасности сетей и систем связи	2	4		6,8	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
Всего часов:		18	36		53,8		

Семестр А

№	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	ЛР	СРС		
1	2	3	4	5	6	8	9
Модуль 3. Методы и средства защиты информации в системах связи							
1	Правовые и организационные методы защиты информации	2	4		6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
2	Стандарты в области защиты информации	2	4		6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
3	Политика безопасности	2	4		7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
4	Защита информации в радиосетях, телефонных сетях, компьютерных сетях	2	4		6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
Модуль 4. Защита информации в каналах общего пользования							
5	Защита информации в телефонных каналах	2	4		6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы,	Практическая работа, тестирование

						интернет-источников.	
6	Защита информации в каналах сотовой связи	2	4		6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
7	IP-телефония	2	4		6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
8	Защита информации в компьютерных сетях	2	4		6,8	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
Всего часов:		16	32		49,8		