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

Актуализировано:
на заседании кафедры
протокол от «07» июня 2018 г. № 10
Зав. кафедрой /А.С. Исмагилова

Согласовано:
Председатель УМК института
/Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информации в системах связи

Б1.В.1.ДВ.12.02 (вариативная)

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

профиль подготовки
Организация и технология защиты информации

Квалификация
бакалавр

Разработчик (составитель)
старший преподаватель /А.М. Махмутов

Дата приема: 2016 г.

Уфа 2018 г.

Составитель: А.М. Махмутов

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью протокол №10 от «07» июня 2018 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 планируемыми результатами освоения образовательной программы

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	1. общенаучные методы и понятия, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	– способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач (ОПК-1)	
	2. основные понятия и методы математического анализа, теории вероятностей и математической статистики, математической логики и теории алгоритмов, теории информации и кодирования, математические методы обработки экспериментальных данных	– способность применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2)	
	3. основные понятия, законы и модели механики; основные понятия, законы и модели электричества и магнетизма , особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности, основные методы исследования и анализа, применяемые в современной физике и технике, базовые теории классической и современной электротехники, электроники и	– способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3)	

	схемотехники, а также основные законы и принципы, управляющие природными явлениями и процессами, на основе которых работают современные приборы		
	4. принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации, структурное программирование, классификацию систем передачи и приема информации и основные характеристики различных специальных типов сетей связи, технологию построения защищенных компьютерных систем, способы задания множеств, основные операции над ними, отношения между элементами множеств, их свойства и виды отношений, типы технических средств охраны, методы защиты информации и построения политик сетевой безопасности, технические каналы утечки информации в системах связи, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам	– способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3)	
	5. политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие	– способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты	

	системы управления, основные виды структур, принципы системного подхода к анализу структур	информации (ПК-6)	
Умения	1. моделировать и прогнозировать развитие процессов и явлений при решении профессиональных задач с использованием общенаучных методов и понятий, законов физики, математического аппарата	– способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач (ОПК-1)	
	2. использовать математические методы и модели для решения прикладных задач	– способность применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2)	
	3. применять основные законы электротехники, электроники и схемотехники при решении прикладных задач	– способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3)	
	4. осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты безопасности, реализовывать алгоритмы на языке программирования высокого уровня, оценивать защищенность компьютерных систем, определять направления использования системы и сети передачи информации для решения служебных задач, применять положения и методы дискретной математики для решения задач, относящихся к темам дисциплины, эксплуатировать технические средства и	– способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3)	

	системы охраны объектов, анализировать механизмы реализации методов защиты операционных систем, анализировать и оценивать угрозы информационной безопасности в системах связи		
	5. реализовывать на практике принципы политики безопасности, использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	– способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)	
Владения (навыки / опыт деятельности)	1. использования методов моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	– способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач (ОПК-1)	
	2. основными методами исследования функций и навыками формулирования и решения простейших задач об отыскании экстремума функции, навыками анализа алгебраических и геометрических объектов	– способность применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2)	
	3. проведения физического эксперимента и обработки его результатов	– способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3)	
	4. методами и средствами выявления угроз безопасности автоматизированным	– способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3)	

	системам, программированием на языке высокого уровня, методами и средствами выявления угроз безопасности автоматизированным системам, навыками работы с технической документацией по сетям и каналам связи, методами решения задач теории множеств, комбинаторного анализа, теории графов, навыками подготовки отчетов, презентаций, навыками безопасного использования технических средств охраны в профессиональной деятельности, методами технической защиты информации в компьютерных сетях, методами технической защиты информации в системах связи		
	5. анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	– способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)	

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Защита информации в системах связи» относится к дисциплинам вариативной части образовательной программы.

Дисциплина изучается на 3 курсе в 5 семестре.

Цели изучения дисциплины: формирование у специалистов целостного представления об общих закономерностях развития и функционирования систем защиты информации.

Изучение дисциплины базируется на знаниях, умениях и навыках, сформированных в результате освоения студентами предшествующих дисциплин образовательной программы по направлению подготовки 10.03.01 – «Информационная безопасность» профиля «Организация и технология защиты информации»: «Физика», «Информатика».

Освоение дисциплины «Информационно-аналитическая деятельность по обеспечению комплексной безопасности» служит основой для выполнения практических мероприятий по защите информации. Полученные знания, навыки и умения используются при прохождении преддипломной практики и 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 с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

ОПК-1. Способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: основные понятия и задачи в области информационно-коммуникационных технологий для решения стандартных	Имеет фрагментарные знания об основных понятиях в области общенаучных методов, понятия, законы физики, математичес	В целом знает основные понятия и задачи в области информационно-коммуникационных технологий для решения	Знает основные понятия и задачи в области информационно-коммуникационных технологий для решения стандартных	Демонстрирует целостность знания об основных понятиях и задачах в области информационно-коммуникационных

	задач профессиональной деятельности	кий аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	стандартных задач профессиональной деятельности, но допускает значительные ошибки	задач профессиональной деятельности, но допускает незначительные ошибки	технологий для решения стандартных задач профессиональной деятельности
Второй этап (уровень)	Уметь: работать с офисными программами, проводить поиск информации, осуществлять сбор и анализ данных, необходимых для проведения конкретных расчетов; обрабатывать массивы данных в соответствии с поставленной задачей.	Умеет работать и смоделировать, прогнозировать развитие процессов и явлений при решении профессиональных задач с использованием общенаучных методов и понятий, законов физики, математического аппарата	Умеет работать с офисными программами, проводить поиск информации, осуществлять сбор и анализ данных, необходимых для проведения конкретных расчетов; но не умеет обрабатывать массивы данных в соответствии с поставленной задачей.	Уверенно работает с офисными программами, проводить поиск информации, осуществлять сбор и анализ данных, необходимых для проведения конкретных расчетов; обрабатывать массивы данных в соответствии с поставленной задачей, но допускает незначительные ошибки.	Уверенно работает с офисными программами, проводить поиск информации, осуществлять сбор и анализ данных, необходимых для проведения конкретных расчетов; обрабатывать массивы данных в соответствии с поставленной задачей.
Третий этап (уровень)	Владеть: информационно-коммуникационными технологиями с учетом основных требований информационной безопасности.	Не способен выбрать необходимые для работы информационно-коммуникационные технологии.	Владеет способностью выбора информационно-коммуникационными технологий, но без учета основных требований информационной безопасности	Владеет способностью аргументированного выбора информационно-коммуникационными технологиями, но испытывает незначительные трудности	Владеет способностью выбора и использования информационно-коммуникационными технологиями с учетом основных требований информационной

				при обеспечении информационной безопасности.	безопасности.

ОПК-2. Способность применять соответствующий математический аппарат для решения профессиональных задач.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать основные понятия и методы математического анализа, теории вероятностей и математической статистики, математической логики и теории алгоритмов, теории информации и кодирования, математические методы обработки экспериментальных данных	Имеет фрагментарные знания об основных понятиях и методах математического анализа, теории вероятностей и математической статистики, математической логики и теории алгоритмов, теории информации и кодирования, математические методы обработки экспериментальных данных	Знает об основных понятиях и методах математического анализа, теории вероятностей и математической статистики, математической логики и теории алгоритмов, теории информации и кодирования, математические методы обработки экспериментальных данных, однако допускает значительные ошибки при их интерпретации	Знает об основных понятиях и методах математического анализа, теории вероятностей и математической статистики, математической логики и теории алгоритмов, теории информации и кодирования, математические методы обработки экспериментальных данных, однако допускает незначительные ошибки при их интерпретации	Знает об основных понятиях и методах математического анализа, теории вероятностей и математической статистики, математической логики и теории алгоритмов, теории информации и кодирования, математические методы обработки экспериментальных данных

Второй этап (уровень)	Уметь: использовать математические методы и модели для решения прикладных задач	Не показывает сформированные умения использовать математические методы и модели для решения прикладных задач	Умеет использовать математические методы и модели для решения прикладных задач, но не может применить на практике.	Способен использовать математические методы и модели для решения прикладных задач.	Аргументировано использует математические методы и модели для решения прикладных задач
Третий этап (уровень)	Владеть основными методами исследования функций и навыками формулирования и решения простейших задач об отыскании экстремума функции, навыками анализа алгебраических и геометрических объектов	Отсутствуют навыки работы с основными методами исследования функций и навыками формулирования и решения простейших задач об отыскании экстремума функции, навыками анализа алгебраических и геометрических объектов	В целом владеет навыками работы с основными методами исследования функций и навыками формулирования и решения простейших задач об отыскании экстремума функции, навыками анализа алгебраических и геометрических объектов, но допускает значительные ошибки	В целом владеет навыками работы с основными методами исследования функций и навыками формулирования и решения простейших задач об отыскании экстремума функции, навыками анализа алгебраических и геометрических объектов, но допускает незначительные ошибки при анализе системы безопасности	Владеет навыками работы с основными методами исследования функций и навыками формулирования и решения простейших задач об отыскании экстремума функции, навыками анализа алгебраических и геометрических объектов

ОПК-3. способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)

	компетенций)				
Первый этап (уровень)	Знать: основные понятия, законы и модели механики; основные понятия, законы и модели электричества и магнетизма , особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности, основные методы исследования и анализа, применяемые в современной физике и технике, базовые теории классической и современной электротехники, электроники и схемотехники , а также основные законы и принципы, управляющие природными явлениями и процессами, на основе которых работают	Имеет фрагментарные знания об основных понятиях, законах и модели механики; основные понятия, законы и модели электричества и магнетизма , особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности , основные методы исследования и анализа, применяемые в современной физике и технике, базовые теории классической и современной электротехники, электроники и схемотехники, а также основные законы и принципы, управляющие природными	В целом знает основные понятия, законы и модели механики; основные понятия, законы и модели электричества и магнетизма , особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности , основные методы исследования и анализа, применяемые в современной физике и технике, базовые теории классической и современной электротехники, электроники и схемотехники, а также основные законы и принципы, управляющие природными явлениями и	Знает основные понятия, законы и модели механики; основные понятия, законы и модели электричества и магнетизма , особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности , основные методы исследования и анализа, применяемые в современной физике и технике, базовые теории классической и современной электротехники, электроники и схемотехники, а также основные законы и принципы, управляющие природными явлениями и процессами,	Знает основные понятия, законы и модели механики; основные понятия, законы и модели электричества и магнетизма , особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности , основные методы исследования и анализа, применяемые в современной физике и технике, базовые теории классической и современной электротехники, электроники и схемотехники, а также основные законы и принципы, управляющие природными явлениями и процессами,

	современные приборы	явлениями и процессами, на основе которых работают современные приборы	процессами, на основе которых работают современные приборы, но допускает значительные ошибки	на основе которых работают современные приборы но допускает незначительные ошибки	на основе которых работают современные приборы
Второй этап (уровень)	Уметь: применять основные законы электротехники, электроники и схемотехники при решении прикладных задач	Не показывает сформированные умения в применении основных законов электротехники, электроники и схемотехники при решении прикладных задач информации	Ориентируется в работе по применению основных законов электротехники, электроники и схемотехники при решении прикладных задач	Способен использовать в работе по применению основных законов электротехники, электроники и схемотехники при решении прикладных задач	Уверенно использует в работе по применению основных законов электротехники, электроники и схемотехники при решении прикладных задач
Третий этап (уровень)	Владеть: проведения физического эксперимента и обработки его результатов	Не способен провести физический эксперимент и обработать его результатов	В целом владеет навыками проведения физического эксперимента и обработки его результатов, но допускает значительные ошибки	Владеет методикой проведения физического эксперимента и обработки его результатов, но испытывает незначительные трудности при определении путей реализации угроз	Владеет методикой проведения физического эксперимента и обработки его результатов

ПК-3. способность администрировать подсистемы информационной безопасности объекта защиты.

Этап (уровень)	Планируемые результаты	Критерии оценивания результатов обучения			
		2 («Не	3	4	5

освоения компетенции	обучения (показатели достижения заданного уровня освоения компетенций)	удовлетворительно»)	(«Удовлетворительно»)	(«Хорошо»)	(«Отлично»)
Первый этап (уровень)	Знать: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации, структурное программирование, классификацию систем передачи и приема информации и основные характеристики различных специальных типов сетей связи, технологию построения защищенных компьютерных систем, способы задания множеств, основные операции над ними, отношения между элементами множеств, их	Фрагментарные представления о принципах и методах противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации, структурное программирование, классификацию систем передачи и приема информации и основные характеристики различных специальных типов сетей связи, технологию построения защищенных компьютерных систем, способы задания множеств, основные операции над ними,	В целом успешные, но не систематические представления о принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации, структурное программирование, классификацию систем передачи и приема информации и основные характеристики различных специальных типов сетей связи, технологию построения защищенных компьютерных систем, способы задания множеств, основные	В целом успешные, но содержащие отдельные пробелы, представления о принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации, структурное программирование, классификацию систем передачи и приема информации и основные характеристики различных специальных типов сетей связи, технологию построения защищенных компьютерных систем, способы задания множеств,	Сформированные представления о принципах и методах противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации, структурное программирование, классификацию систем передачи и приема информации и основные характеристики различных специальных типов сетей связи, технологию построения защищенных компьютерных систем, способы задания множеств, основные операции над ними,

	свойства и виды отношений, типы технических средств охраны, методы защиты информации и построения политик сетевой безопасности, технические каналы утечки информации в системах связи, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам	отношения между элементами множеств, их свойства и виды отношений, типы технических средств охраны, методы защиты информации и построения политик сетевой безопасности, технические каналы утечки информации в системах связи, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам	операции над ними, отношения между элементами множеств, их свойства и виды отношений, типы технических средств охраны, методы защиты информации и построения политик сетевой безопасности, технические каналы утечки информации в системах связи, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам	основные операции над ними, отношения между элементами множеств, их свойства и виды отношений, типы технических средств охраны, методы защиты информации и построения политик сетевой безопасности, технические каналы утечки информации в системах связи, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам	отношения между элементами множеств, их свойства и виды отношений, типы технических средств охраны, методы защиты информации и построения политик сетевой безопасности, технические каналы утечки информации в системах связи, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам
Второй этап (уровень)	Уметь: осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Слабо выраженные способности осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программны	Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных	Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных	Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных

	безопасности, реализовывать алгоритмы на языке программирования высокого уровня, оценивать защищенность компьютерных систем, определять направления использования системы и сети передачи информации для решения служебных задач, применять положения и методы дискретной математики для решения задач, относящихся к темам дисциплины, эксплуатировать технические средства и системы охраны объектов, анализировать механизмы реализации методов защиты операционных систем, анализировать и оценивать угрозы информационной	х и аппаратных средств защиты безопасности, реализовывать алгоритмы на языке программирования высокого уровня, оценивать защищенность компьютерных систем, определять направления использования системы и сети передачи информации для решения служебных задач, применять положения и методы дискретной математики для решения задач, относящихся к темам дисциплины, эксплуатировать технические средства и системы охраны объектов, анализировать механизмы реализации методов защиты операционных систем,	средств защиты безопасности, реализовывать алгоритмы на языке программирования высокого уровня, оценивать защищенность компьютерных систем, определять направления использования системы и сети передачи информации для решения служебных задач, применять положения и методы дискретной математики для решения задач, относящихся к темам дисциплины, эксплуатировать технические средства и системы охраны объектов, анализировать механизмы реализации методов защиты операционных систем, анализировать и оценивать	средств защиты безопасности, реализовывать алгоритмы на языке программирования высокого уровня, оценивать защищенность компьютерных систем, определять направления использования системы и сети передачи информации для решения служебных задач, применять положения и методы дискретной математики для решения задач, относящихся к темам дисциплины, эксплуатировать технические средства и системы охраны объектов, анализировать механизмы реализации методов защиты операционных систем, анализировать и оценивать	средств защиты безопасности, реализовывать алгоритмы на языке программирования высокого уровня, оценивать защищенность компьютерных систем, определять направления использования системы и сети передачи информации для решения служебных задач, применять положения и методы дискретной математики для решения задач, относящихся к темам дисциплины, эксплуатировать технические средства и системы охраны объектов, анализировать механизмы реализации методов защиты операционных систем, анализировать и оценивать

	безопасности в системах связи	анализировать и оценивать угрозы информационной безопасности в системах связи	угрозы информационной безопасности в системах связи, но с пробелами умения интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных, разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	угрозы информационной безопасности в системах связи, но имеются не большие недочеты	угрозы информационной безопасности в системах связи
Третий этап (уровень)	Владеть: методами и средствами выявления угроз безопасности автоматизированным системам, программированием на языке высокого уровня, методами и средствами выявления угроз безопасности	Фрагментарные навыки использования методов и средств выявления угроз безопасности автоматизированным системам, программированием на языке высокого уровня, методами и средствами выявления	В целом успешные, но не использования методов и средств выявления угроз безопасности автоматизированным системам, программированием на языке высокого уровня, методами и средствами	В целом успешное, но содержащее отдельные пробелы навыки использования методов и средств выявления угроз безопасности автоматизированным системам, программированием на языке высокого	Успешное и систематическое применение навыков использования методов и средств выявления угроз безопасности автоматизированным системам, программированием на языке высокого уровня,

	автоматизированным системам, навыками работы с технической документацией по сетям и каналам связи, методами решения задач теории множеств, комбинаторного анализа, теории графов, навыками подготовки отчетов, презентаций, навыками безопасного использования технических средств охраны в профессиональной деятельности, методами технической защиты информации в компьютерных сетях, методами технической защиты информации в системах связи	угроз безопасности автоматизированным системам, навыками работы с технической документацией по сетям и каналам связи, методами решения задач теории множеств, комбинаторного анализа, теории графов, навыками подготовки отчетов, презентаций, навыками безопасного использования технических средств охраны в профессиональной деятельности, методами технической защиты информации в компьютерных сетях, методами технической защиты информации в системах связи	выявления угроз безопасности автоматизированным системам, навыками работы с технической документацией по сетям и каналам связи, методами решения задач теории множеств, комбинаторного анализа, теории графов, навыками подготовки отчетов, презентаций, навыками безопасного использования технических средств охраны в профессиональной деятельности, методами технической защиты информации в компьютерных сетях, методами технической защиты информации в системах связи	уровня, методами и средствами выявления угроз безопасности автоматизированным системам, навыками работы с технической документацией по сетям и каналам связи, методами решения задач теории множеств, комбинаторного анализа, теории графов, навыками подготовки отчетов, презентаций, навыками безопасного использования технических средств охраны в профессиональной деятельности, методами технической защиты информации в компьютерных сетях, методами технической защиты информации в системах связи	методами и средствами выявления угроз безопасности автоматизированным системам, навыками работы с технической документацией по сетям и каналам связи, методами решения задач теории множеств, комбинаторного анализа, теории графов, навыками подготовки отчетов, презентаций, навыками безопасного использования технических средств охраны в профессиональной деятельности, методами технической защиты информации в компьютерных сетях, методами технической защиты информации в системах связиа

ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	Имеет фрагментарные знания о политике, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	В целом знает основные политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур, но допускает значительные ошибки.	Хорошо знает основные политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур, но допускает незначительные ошибки.	Демонстрирует целостность знаний политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур
Второй этап (уровень)	Уметь: реализовывать на практике принципы политики безопасности, использовать методы количественного	Не умеет реализовывать на практике принципы политики безопасности, использовать методы количественн	Умеет применять реализовывать на практике принципы политики безопасности, использовать методы	Умеет реализовывать на практике принципы политики безопасности, использовать методы количественн	Умеет эффективно реализовывать на практике принципы политики безопасности, использовать методы

	представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	ого представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности, но не умеет интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих источниках	ого представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности, но допускает незначительные ошибки.	количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности
Третий этап (уровень)	Владеть анализом, обработкой и интерпретацией результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной	Не способен провести анализ, обработку и интерпретацию результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информацио	Владеет методиками анализа, обработкой и интерпретацией результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информацио	Владеет методиками анализа, обработкой и интерпретацией результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информацио	Владеет методиками анализа, обработкой и интерпретацией результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информацио

	безопасность ю, организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	нной безопасность ю, организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	нной безопасность ю, организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации, но без анализа и интерпретации информации, содержащейся в различных источниках	нной безопасность ю, организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	нной безопасность ю, организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации

4.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
1-й этап Знания	1. общенаучные методы и понятия, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	– способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач (ОПК-1)	Устный индивидуальный опрос, групповой опрос, тестирование, творческое задание
	2. основные понятия и методы математического анализа, теории вероятностей и	– способность применять соответствующий математический аппарат для решения	Устный индивидуальный опрос, групповой

	математической статистики, математической логики и теории алгоритмов, теории информации и кодирования, математические методы обработки экспериментальных данных	профессиональных задач (ОПК-2)	опрос, тестирование, творческое задание
	3. основные понятия, законы и модели механики; основные понятия, законы и модели электричества и магнетизма , особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности, основные методы исследования и анализа, применяемые в современной физике и технике, базовые теории классической и современной электротехники, электроники и схемотехники, а также основные законы и принципы, управляющие природными явлениями и процессами, на основе которых работают современные приборы	– способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3)	Устный индивидуальный опрос, групповой опрос, тестирование, творческое задание
	4. принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации, структурное программирование, классификацию систем передачи и приема информации и основные характеристики различных специальных типов сетей связи,	– способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3)	Устный индивидуальный опрос, групповой опрос, тестирование, творческое задание

	технологию построения защищенных компьютерных систем, способы задания множеств, основные операции над ними, отношения между элементами множеств, их свойства и виды отношений, типы технических средств охраны, методы защиты информации и построения политик сетевой безопасности, технические каналы утечки информации в системах связи, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам		
	5. политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	– способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)	Устный индивидуальный опрос, групповой опрос, тестирование, творческое задание
2-й этап Умения	1. моделировать и прогнозировать развитие процессов и явлений при решении профессиональных задач с использованием общенаучных методов и понятий, законов физики, математического аппарата	– способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач (ОПК-1)	Устный индивидуальный опрос, групповой опрос, тестирование, творческое задание
	2. использовать	– способность применять	Устный

	математические методы и модели для решения прикладных задач	соответствующий математический аппарат для решения профессиональных задач (ОПК-2)	индивидуальный опрос, групповой опрос, тестирование, творческое задание
	3. применять основные законы электротехники, электроники и схемотехники при решении прикладных задач	– способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3)	Устный индивидуальный опрос, групповой опрос, тестирование, творческое задание
	4. осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты безопасности, реализовывать алгоритмы на языке программирования высокого уровня, оценивать защищенность компьютерных систем, определять направления использования системы и сети передачи информации для решения служебных задач, применять положения и методы дискретной математики для решения задач, относящихся к темам дисциплины, эксплуатировать технические средства и системы охраны объектов, анализировать механизмы реализации методов защиты операционных систем, анализировать и оценивать угрозы информационной безопасности в системах связи	– способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3)	Устный индивидуальный опрос, групповой опрос, тестирование, творческое задание

	5. реализовывать на практике принципы политики безопасности, использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	– способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)	Устный индивидуальный опрос, групповой опрос, тестирование, творческое задание
3-й этап Владения навыками	1. использования методов моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	– способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач (ОПК-1)	Устный индивидуальный опрос, групповой опрос, тестирование, творческое задание
	2. основными методами исследования функций и навыками формулирования и решения простейших задач об отыскании экстремума функции, навыками анализа алгебраических и геометрических объектов	– способность применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2)	Устный индивидуальный опрос, групповой опрос, тестирование, творческое задание
	3. проведения физического эксперимента и обработки его результатов	– способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач (ОПК-3)	Устный индивидуальный опрос, групповой опрос, тестирование, творческое задание
	4. методами и средствами выявления угроз безопасности автоматизированным системам,	– способность администрировать подсистемы информационной безопасности объекта	Устный индивидуальный опрос, групповой опрос,

	программированием на языке высокого уровня, методами и средствами выявления угроз безопасности автоматизированным системам, навыками работы с технической документацией по сетям и каналам связи, методами решения задач теории множеств, комбинаторного анализа, теории графов, навыками подготовки отчетов, презентаций, навыками безопасного использования технических средств охраны в профессиональной деятельности, методами технической защиты информации в компьютерных сетях, методами технической защиты информации в системах связи	защиты (ПК-3)	тестирование, творческое задание
	5. анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	– способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6)	Устный индивидуальный опрос, групповой опрос, тестирование, творческое задание

4.3. Рейтинг-план дисциплины (при необходимости)

Рейтинг–план дисциплины представлен в приложении 2.

Экзамен

Структура экзаменационного билета: экзаменационный билет состоит из двух вопросов, отражающих соответственно материал первого и второго модуля.

Типовые экзаменационные материалы

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. Утечка информации по системам электропитания и заземления.
9. Технические каналы утечки информации.
10. Акустические каналы утечки информации.
11. Оптические каналы утечки информации.
12. Радиоэлектронные каналы утечки информации.
13. Методы и средства защиты информации от ее утечки по техническим каналам.

Пример экзаменационного билета:

Форма 1.4.-33

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Направление подготовки 10.03.01 Информационная безопасность

Дисциплина Защита информации в системах связи

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1 Демаскирующие признаки сигналов..
2 Электромагнитные излучения распределенных источников.

Зав. кафедрой управления
информационной безопасностью А.С. Исмагилова

Кафедра управления информационной безопасностью

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.

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.
- 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. Студент не смог ответить ни на один дополнительный вопрос

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.

Тестирование

1. К принципам обеспечения безопасности относится:
а) согласованность;
б) взаимная ответственность личности, общества и государства;
в) децентрализации и демократизм.

2. 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.

3. Не являются видами угроз информационной безопасности:
а) внутренние угрозы;
б) внешние угрозы;
в) значительные угрозы.

4. Не являются видами угроз информационной безопасности:
а) угрозы военные;
б) угрозы потенциальные;

в) угрозы реальные.

5. К методам обеспечения информационной безопасности Российской Федерации относятся:
а) правовые;
б) неправовые;
в) легальные.

6. К методам обеспечения информационной безопасности Российской Федерации относятся:
а) методы принуждения;
б) организационно-технические;
в) секретные.

7. К методам обеспечения информационной безопасности Российской Федерации относятся:
а) оперативные;
б) конструктивные;
в) экономические.

8. Сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации это:
а) сфера хранения информации;
б) информационная сфера;
в) сфера государственного регулирования информации.

Критерии оценивания теста

В комплекте тестов 25 вопросов,
за один правильный ответ ставится 0.4 балла.
За тест максимальный балл 10 баллов

Творческое задание (презентация, доклад)

Выполняется по результатам изучения темы дисциплины с целью дополнения практического материала.

Примеры тем творческих заданий:

1. Законодательная база в области защиты информации.
2. Структура государственных органов обеспечивающих защиту информации.
3. Общая характеристика организационных методов ЗИ.
4. Общие критерии безопасности информации.
5. Действующие стандарты РФ по защите информации.
6. Понятие политики безопасности.
7. Уязвимости. Модели основных политик от НСД.
8. Особенности защиты информации в системах связи.
9. Криптография.
10. Стеганография.
11. Защита компьютерных сетей.

Критерии и методика оценивания:
Подготовленная и оформленная в соответствии с требованиями работа (презентация, доклад) оценивается преподавателем по следующим критериям:

- уровень эрудированности автора по изученной теме (знание автором состояния изучаемой проблематики, цитирование источников, в т.ч. НПА);
- логичность подачи материала, грамотность автора;
- соответствие работы всем стандартным требованиям к оформлению;
- знания и умения на уровне требований стандарта данной дисциплины: знание фактического материала, усвоение общих понятий и идей.
- 0 баллов выставляется студенту, если работа не соответствует критериям;
- 1 балл выставляется студенту, если работа частично соответствует критериям;
- 3 балла выставляется студенту, если работа соответствует критериям, но отсутствует логичность изложения информации;
– 5 баллов выставляется студенту, если работа полностью соответствует критериям.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература:

1. 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
2. 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
3. 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

Дополнительная литература:

4. Аверченков, В.И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356
5. Семь безопасных информационных технологий [Электронный ресурс] : учебник / А.В. Барабанов [и др.] ; под ред. Маркова А.С.. — Электрон. дан. — Москва : ДМК Пресс, 2017. — 224 с. — Режим доступа: https://e.lanbook.com/book/97352. — Загл. с экрана.

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

1. Справочная правовая система «КонсультантПлюс» – http://www.consultant-plus.ru.
2. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
3. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
4. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
5. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
6. http://univertv.ru/video/ – 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);
7. www.newlibrary.ru – Новая электронная библиотека;
8. www. edu.ru – Федеральный портал российского образования;
9. www.elibrary.ru – Научная электронная библиотека;
10. www.nehudlit.ru – Электронная библиотека учебных материалов.
11. 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.
12. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
13. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения	
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***	Лекции, практические занятия, лабораторные занятия, групповые и индивидуальные консультации, 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 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-	1. 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. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.

проведения лабораторных работ: компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **3.** ***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). **4.** ***учебная аудитория для проведения групповых и индивидуальных консультаций:*** 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). **5.** ***учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 403 (гуманитарный корпус), аудитория № 415		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. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт APAPT 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 APAPT 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 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	3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

(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:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **7.*помещение для хранения и профилактического обслуживания учебного оборудования:***аудитория № 523 (гуманитарный корпус).		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

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины Защита информации в системах связи
на 5 семестр

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	37,2
лекций	18
практических / семинарских	18
лабораторных	-
контроль самостоятельной работы (КСР)	
форма контактной работы (ФКР)	
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	1,2
Учебных часов на самостоятельную работу обучающихся, включая подготовку к экзамену	45 25,8

Форма контроля
Экзамен 5 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / Сем	ЛР	СРС			
1	2	4	5	6	7	8	9	10
Модуль 1. **Основные понятия и положения защиты информации в системах связи**								
1	Введение в дисциплину	2	2	-	5	1-3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Устный опрос, тест, творческое задание
2	Угрозы безопасности информации.	2	2	-	5	1-5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Устный опрос, тест, творческое задание
3	Злоумышленники угроз.	2	2	-	5	1-4	Самостоятельное изучение рекомендуемой основной и дополнительной	Устный опрос, тест, творческое задание

							литературы, интернет-источников.	
4	Основные принципы ЗИвСС.	3	3	-	5	1-5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Устный опрос, тест, творческое задание
Модуль 2. **Методы и средства защиты информации в системах связи**								
1	Правовые и организационные методы защиты информации	2	2	-	6	1-3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Устный опрос, тест, творческое задание
2	Стандарты в области защиты информации	2	2	-	6	1-5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Устный опрос, тест, творческое задание
3	Политика безопасности	2	2	-	6	1-5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Устный опрос, тест, творческое задание
4	Защита	3	3	-	7	1-5	Самостоятельное	Устный опрос,

	информации в радиосетях, телефонных сетях, компьютерных сетях						изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	тест, творческое задание
	итого	18	18		45			

Приложение 2

Рейтинг – план дисциплины

Защита информации в системах связи

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. Творческое задание	1	5	0	5
3. Практические работы	3	5	0	15
Рубежный контроль				10
1. Тестовые задания	0,4	25	0	10
Всего			0	35
Модуль 2				
Текущий контроль			0	25
1. Аудиторная работа	1	5	0	5
2. Творческое задание	1	5	0	5
3. Практические работы	3	5	0	15
Рубежный контроль				10
1. Тестовые задания	0,4	25	0	10
Всего			0	35
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 занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Экзамен			0	30