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 информационных процессов в компьютерных системах

Б1.В.1.ДВ.10.01 вариативная

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации

Квалификация
бакалавр

Разработчики (составители)
старший преподаватель /А.А. Ахмеров
ассистент /А.Ф. Фатхелисламов

Для приема: 2016 г.

Уфа 2018 г.

Составители: А.А. Ахмеров, А.Ф. Фатхелисламов

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/

Содержание

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. представление об администрировании подсистем информационной безопасности компьютерных систем; 2. представление об аттестации объектов, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации; 3. представление о проведении проектных расчетов элементов систем обеспечения информационной безопасности компьютерных систем; 4. представление о контроле эффективности реализации политики информационной безопасности компьютерных систем;	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1); способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2); способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3); способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5); способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6); способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10); способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)	

Умения	1. вести сбор и анализ исходных данных для проектирования систем защиты информации для компьютерных систем, определения требований, сравнительного анализа подсистем по показателям информационной безопасности;2	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1); способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2); способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3); способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5); способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6); способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10); способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)	
Владения (навыки / опыт деятельности)	1. навыками проведения предварительного технико-экономического обоснования проектных расчетов; 2. навыками установки, настройки, эксплуатации и поддержания в работоспособном состоянии компонентов системы обеспечения информационной безопасности компьютерных систем с	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1); способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2); способность администрировать подсистемы	

	учетом установленных требований;	информационной безопасности объекта защиты (ПК-3); способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5); способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6); способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10); способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)	

2. Цель и место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Защита информационных процессов в компьютерных системах» относится к базовой части образовательной программы.

Дисциплина изучается на 4-ом курсе в 7-ом семестре.

Цели изучения дисциплины: формирование у бакалавров целостного представления о защите информации и информационных системах.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин:

Аппаратные средства вычислительной техники,
Программно-аппаратные средства защиты информации,
Криптографические методы защиты информации,
Техническая защита информации,
Технические средства охраны,
Техническая радиоэлектронная разведка,
Системы инженерно-технической защиты информации,
Защита информационных процессов в компьютерных системах,
Противодействие речевой (акустической) разведке

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

ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) 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: аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД; эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информацион	Не знает	Имеет фрагментарные знания об аппаратных средствах вычислительной техники; операционных системах персональных ЭВМ; основах администрирования вычислительных сетей; системах управления БД; эксплуатационных и технико-экономических характеристиках программных и технических средств	В целом знает основные понятия об аппаратных средствах вычислительной техники; операционных системах персональных ЭВМ; основах администрирования вычислительных сетей; системах управления БД; эксплуатационных и технико-экономических характеристиках программных и технических	Демонстрирует целостность знания об об аппаратных средствах вычислительной техники; операционных системах персональных ЭВМ; основах администрирования вычислительных сетей; системах управления БД; эксплуатационных и технико-экономических характеристиках программных и технических

	ной безопасности; типы технических и программно-аппаратных средств обработки и защиты информации		защиты информации и обеспечения информационной безопасности; типах технических и программно-аппаратных средств обработки и защиты информации	средств защиты информации и обеспечения информационной безопасности; типах технических и программно-аппаратных средств обработки и защиты информации, но допускает значительные ошибки	средств защиты информации и обеспечения информационной безопасности; типах технических и программно-аппаратных средств обработки и защиты информации
Второй этап (уровень)	Уметь: формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; выполнять работы по	Не умеет	Умеет формулировать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	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.

	установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации				
Третий этап (уровень)	Владеть: методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации	Не владеет	Владеет методами тестирования средств программно-технического обеспечения защиты информации	Владеет методами оценки, тестирования . настройки на применение средств программно-технического обеспечения защиты информации, но без учета основных требований информационной безопасности	Владеет методами оценки, тестирования . настройки на применение средств программно-технического обеспечения защиты информации с учетом основных требований информационной безопасности

ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования 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: основы систем и языков программирования; инструментальные средства для обработки данных; средства разработки программного обеспечения; технологии создания программ сложной структуры	Не знает	В целом знает основы систем и языков программирования, инструментальные средства для обработки данных; средства разработки программного обеспечения, технологии создания программ сложной структуры, но допускает значительные ошибки	Знает основы систем и языков программирования, инструментальные средства для обработки данных; средства разработки программного обеспечения, технологии создания программ сложной структуры, но допускает незначительные ошибки	Знает основы систем и языков программирования, инструментальные средства для обработки данных; средства разработки программного обеспечения, технологии создания программ сложной структуры
Второй этап (уровень)	Уметь: использовать существующие пакеты прикладных программ для решения поставленной задачи; реализовать и отлаживать пакеты прикладных программ; решать задачи проектирования программных систем с помощью различных методов	Не умеет	Умеет использовать существующие пакеты прикладных программ для решения поставленной задачи, но не умеет их разрабатывать пакеты и решать задачи проектирования программных систем с помощью различных методов	Уверенно использует существующие пакеты прикладных программ для решения поставленной задачи; реализует и отлаживает пакеты прикладных программ, но возникают сложности с решением задач проектирования программных систем с помощью различных методов	Уверенно использует существующие пакеты прикладных программ для решения поставленной задачи; реализует и отлаживает пакеты прикладных программ; решает задачи проектирования программных систем с помощью различных методов

Третий этап (уровень)	Владеть: навыками применения инструментальных средств для создания программ различного назначения; навыками создания системного, прикладного ПО для решения профессиональных задач	Не владеет	Владеет навыками применения инструментальных средств для создания программ различного назначения; навыками создания системного, прикладного ПО для решения профессиональных задач, но допускает значительные ошибки	Уверенно применяет инструментальные средства для создания программ различного назначения; возникают небольшие сложности при создании системного, прикладного ПО.	Владеет навыками применения инструментальных средств для создания программ различного назначения; навыками создания системного, прикладного ПО для решения профессиональных задач

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

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: методы и средства управления защитой информации в операционных системах, базах данных и прикладных программах; настройки и конфигурирования программных средства борьбы со злонамеренным	Не знает	В целом знает основные методы и средства управления защитой информации в операционных системах, базах данных и прикладных программах.	Знает основные методы и средства управления защитой информации в операционных системах, базах данных и прикладных программах; настройки и конфигурирования программны	Демонстрирует целостность знания об методах и средствах управления защитой информации в операционных системах, базах данных и прикладных программах; настройке и конфигуриро

	программным обеспечением; характеристики аппаратных средств борьбы с утечкой информации.			х средства борьбы со злонамеренным программным обеспечением; характеристики аппаратных средств борьбы с утечкой информации.	вании программных средств борьбы со злонамеренным программным обеспечением; характеристике аппаратных средств борьбы с утечкой информации
Второй этап (уровень)	Уметь: настраивать, конфигурировать и использовать средства защиты информации в СУБД, ОС и прикладных программах, используемых в организации; настраивать антивирусные программы и другие средства борьбы с программными закладками, тестировать и настраивать на применение технические средства защиты данных	Не умеет	Умеет настраивать, конфигурировать и использовать средства защиты информации в СУБД, ОС и прикладных программах, используемых в организации;	Умеет настраивать, конфигурировать и использовать средства защиты информации в СУБД, ОС и прикладных программах, используемых в организации; настраивать антивирусные программы и другие средства борьбы с программными закладками, тестировать и настраивать на применение технические средства защиты данных	Свободное умение настраивать, конфигурировать и использовать средства защиты информации в СУБД, ОС и прикладных программах, используемых в организации; настраивать антивирусные программы и другие средства борьбы с программными закладками, тестировать и настраивать на применение технические средства защиты данных

Третий этап (уровень)	Владеть: навыками анализа и оценки угроз информационной безопасности объекта	Не владеет	Фрагментарные навыки анализа и оценки угроз информационной безопасности объекта	Владеет навыками анализа и оценки угроз информационной безопасности объекта, но допускает незначительные ошибки.	Владеет навыками анализа и оценки угроз информационной безопасности объекта.

ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

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; общеметодологические принципы	Не знает	В целом сформированные, но неполные знания о политиках, стратегиях и технологиях информационной безопасности и защиты информации, основных понятиях в области информационной безопасности, возможностях организационных, аппаратных и программны	Сформированные, но содержащие отдельные пробелы знания о политиках, стратегиях и технологиях информационной безопасности и защиты информации, способах их организации и оптимизации; понятиях системы управления, основных видах структур, принципах системного	Сформированные систематические знания о политиках, стратегиях и технологиях информационной безопасности и защиты информации, способах их организации и оптимизации; понятиях системы управления, основных видах структур, принципах системного подхода к

	теории информационной безопасности; возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации; состояние законодательной базы и стандарты в области информационной безопасности, общеметодологические принципы теории информационной безопасности; состояние законодательной базы и стандарты в области информационной безопасности;		х средств безопасности и защиты информации; состоянии законодательной базы и стандартов в области информационной безопасности, общеметодологических принципах теории информационной безопасности; состоянии законодательной базы и стандарты в области информационной безопасности	подхода к анализу структур; общеметодологических принципах теории информационной безопасности; возможностях и особенностях организационных, аппаратных и программных средств безопасности и защиты информации; состоянии законодательной базы и стандартов в области информационной безопасности, общеметодологических принципах теории информационной безопасности; состоянии законодательной базы и стандарты в области информационной безопасности	анализу структур; общеметодологических принципах теории информационной безопасности; возможностях и особенностях организационных, аппаратных и программных средств безопасности и защиты информации; состоянии законодательной базы и стандартов в области информационной безопасности, общеметодологических принципах теории информационной безопасности; состоянии законодательной базы и стандарты в области информационной безопасности
Второй этап (уровень)	Уметь: реализовывать на практике принципы политики безопасности;	Не умеет	В целом успешное, но не систематическое умение применять	Успешное, но содержащее отдельные пробелы умение	Сформированное умение применять принципы политики безопасности

	использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности; обосновывать организационно-технические мероприятия по защите информации; использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации.		принципы политики безопасности; закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности; обосновывать организационно-технические мероприятия по защите информации; использовать возможности организационных, аппаратных и программных средств безопасности и защиты информации	применять принципы политики безопасности; закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности; обосновывать организационно-технические мероприятия по защите информации; использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	; закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности; обосновывать организационно-технические мероприятия по защите информации; использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации
Третий этап (уровень)	Владеть: навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры,	Не владеет	В целом успешное, но не полное владение навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками	Успешное, но содержащее отдельные пробелы владение навыками анализа, обработки и интерпретации результатов решения прикладных задач	Сформированное владение навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формировани

	практические приемы и пр.) для управления информационной безопасностью; навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации; навыками выявления и устранения угроз информационной безопасности; навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; навыками во внедрении, адаптации и настройке средств защиты прикладных ИС.		формирования комплекса мер для управления информационной безопасностью; навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации; навыками выявления и устранения угроз информационной безопасности; навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; навыками во внедрении, адаптации и настройке средств защиты прикладных ИС.	управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью; навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации; навыками выявления и устранения угроз информационной безопасности; навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; навыками во внедрении, адаптации и настройке средств защиты прикладных ИС.	я комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью; навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации; навыками выявления и устранения угроз информационной безопасности; навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; навыками во внедрении, адаптации и настройке средств защиты прикладных ИС.

ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности 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: Правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства	Не знает	В целом знает об основных правовых нормах и стандартах по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; и правовых основах организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства, но допускает значительные ошибки	Хорошо знает об основных правовых нормах и стандартах по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; и правовых основах организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства, но допускает незначительные ошибки	Обладает целостными знаниями об основных правовых нормах и стандартах по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; и правовых основах организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства.

Второй этап (уровень)	Уметь: Выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации; Применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе; Разрабатывать организационно-распорядительные документы по вопросам защиты информации;	Не умеет	Умеет выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации, применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе, но не в полнее умеет разрабатывать организационно-распорядительные документы по вопросам защиты информации	Умеет выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации, применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе, разрабатывать организационно-распорядительные документы по вопросам защиты информации, но допускает незначительные ошибки.	Уверенно умеет выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации, применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе, разрабатывать организационно-распорядительные документы по вопросам защиты информации
Третий этап (уровень)	Владеть: Навыками работы с нормативными и правовыми актами и навыками лицензирования в области защиты информации; методами сбора и анализа исходных данных для проектирован	Не владеет	Владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации; методами сбора и анализа исходных	Владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации; методами сбора и анализа исходных	Владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации; методами сбора и анализа исходных

	ия систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности		данных для проектирования систем защиты информации, но без учета требований по сравнительному анализу подсистем по показателям информационной безопасности	данных для проектирования систем защиты информации, но испытывает незначительные трудности при определении требований и сравнительном анализе подсистем по показателям информационной безопасно	данных для проектирования систем защиты информации, определением требований, сравнительным анализом подсистем по показателям информационной безопасности

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: основные принципы оценки работоспособности и тестирования оборудования обработки и передачи данных; критерии и меры надежности, возможности и особенности организацион	Не знает	В целом знает: об основных принципах оценки работоспособности и тестирования оборудования обработки и передачи данных, но не знает критерии и меры надежности, возможности	Знает: об основных принципах оценки работоспособности и тестирования оборудования обработки и передачи данных; критерии и меры надежности, возможности и особенности	Демонстрирует целостность знания об основных принципах оценки работоспособности и тестирования оборудования обработки и передачи данных; критерии и меры надежности,

	ных, аппаратных и программных средств безопасности и защиты информации		и особенности организационно, аппаратных и программных средств безопасности и защиты информации.	организационных, аппаратных и программных средств безопасности и защиты информации, но допускает незначительные ошибки.	возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации
Второй этап (уровень)	Уметь: использовать возможности и особенности организационных, аппаратных и программных средств обеспечения безопасности и защиты информации; составлять и реализовывать планы тестирующих мероприятий, в том числе имитирующих внешние и внутренние атаки, нарушающие систему информационной безопасности.	Не умеет	Умеет использовать возможности и особенности организационно, аппаратных и программных средств обеспечения безопасности и защиты информации, но не умеет составлять и реализовывать планы тестирующих мероприятий, в том числе имитирующих внешние и внутренние атаки, нарушающие систему информационной безопасности.	Уверенно использует возможности и особенности организационных, аппаратных и программных средств обеспечения безопасности и защиты информации; составлять и реализовывать планы тестирующих мероприятий, в том числе имитирующих внешние и внутренние атаки, нарушающие систему информационной безопасности, но допускает незначительные ошибки.	Уверенно использует возможности и особенности организационных, аппаратных и программных средств обеспечения безопасности и защиты информации; составлять и реализовывать планы тестирующих мероприятий, в том числе имитирующих внешние и внутренние атаки, нарушающие систему информационной безопасности.
Третий этап (уровень)	Владеть: навыками эксплуатации современного электронного оборудования и информацион	Не владеет	Владеет навыками эксплуатации современного электронного оборудования и	Владеет навыками эксплуатации современного электронного оборудования и	Владеет навыками эксплуатации современного электронного оборудования и

	но-коммуникационных технологий; использования методов тестирования коммуникационного оборудования и аппаратуры обработки данных, криптографических систем		информационно-коммуникационных технологий, но не использует методов тестирования коммуникационного оборудования и аппаратуры обработки данных, криптографических систем.	информационно-коммуникационных технологий; использования методов тестирования коммуникационного оборудования и аппаратуры обработки данных, криптографических систем, но испытывает незначительные трудности	информационно-коммуникационных технологий; использования методов тестирования коммуникационного оборудования и аппаратуры обработки данных, криптографических систем

ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

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: критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов	Не знает	В целом знает основные критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов, но допускает значительны	Хорошо знает основные критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов, но допускает незначительн	Демонстрирует целостность знаний критериев оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов

			е ошибки.	ые ошибки.	
Второй этап (уровень)	Уметь: использовать возможности и особенности организационных, аппаратных и программных средств обеспечения безопасности и защиты информации; составлять и реализовывать планы тестирующих мероприятий, в том числе имитирующих внешние и внутренние атаки, нарушающие систему информационной безопасности.	Не умеет	Умеет применять отечественные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; собирать, анализировать информацию, но не умеет интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих источниках	Умеет применять отечественные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих источниках, но допускает незначительные ошибки.	Умеет эффективно применять отечественные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих источниках
Третий этап (уровень)	Владеть: Методиками проверки защищенности объектов информатизации на соответствие требованиям	Не владеет	Владеет методиками проверки защищенности объектов информатизации на соответствие требованиям	Владеет методиками проверки защищенности объектов информатизации на соответствие требованиям	Владеет методиками проверки защищенности объектов информатизации на соответствие требованиям

	нормативных документов; навыками анализа и интерпретации и информации, содержащейся в различных источниках		нормативных документов, но без анализа и интерпретации информации, содержащейся в различных источниках	нормативных документов, но испытывает незначительные трудности при анализе и интерпретации информации, содержащейся в различных источниках	нормативных документов; обладает навыками анализа и интерпретации информации, содержащейся в различных источниках

ПК-12: способность принимать участие в проведении экспериментальных исследований системы 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: основные понятия, виды и принципы экспериментальных исследований; определять цели и задачи проведения экспериментальных исследований	Не знает	В целом знает основные понятия, виды и принципы экспериментальных исследований; но не знает цели и задачи проведения экспериментальных исследований	Знает основные понятия, виды и принципы экспериментальных исследований; определяет цели и задачи проведения экспериментальных исследований, но допускает незначительные ошибки	Знает основные понятия, виды и принципы экспериментальных исследований; определяет цели и задачи проведения экспериментальных исследований
Второй этап (уровень)	Уметь: работать с простейшими приборами,	Не умеет	Умеет работать с простейшими приборами,	Способен работать с простейшими приборами,	Уверенно работает с простейшими приборами,

	схемами, которые могут быть применены при заданной методике эксперимента; понимать принцип их действия; ориентироваться в современной технике и технологиях с целью их освоения и внедрения для решения поставленной задачи		схемами, которые могут быть применены при заданной методике эксперимента, но не понимает суть их работы, не ориентируется в современной технике и технологиях	схемами; понимать принцип их действия; ориентироваться в современной технике и технологиях с целью их освоения и внедрения для решения поставленной задачи, но испытывает трудности со связью теоретических основ и конкретной задачи	схемами, которые могут быть применены при заданной методике эксперимента; понимает принцип их действия; ориентируется в современной технике и технологиях с целью их освоения и внедрения для решения поставленной задачи
Третий этап (уровень)	Владеть: современными инструментальными средствами проведения экспериментов с учетом требований по обеспечению информационной безопасности; навыками анализа экспериментальных результатов	Не владеет	Владеет современными инструментальными средствами проведения экспериментов с учетом требований по обеспечению информационной безопасности и навыками анализа экспериментальных результатов, но допускает значительные ошибки	Владеет современными инструментальными средствами проведения экспериментов с учетом требований по обеспечению информационной безопасности и навыками анализа экспериментальных результатов, но допускает незначительные ошибки	Уверенно владеет современными инструментальными средствами проведения экспериментов с учетом требований по обеспечению информационной безопасности; навыками анализа экспериментальных результатов

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей, перечисленных в рейтинг-плане дисциплины (для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).
Шкалы оценивания для экзамена:
от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;
от 80 баллов – «отлично».

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	Знать аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1); способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2); способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3); способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5); способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности	Контрольная работа, Коллоквиум, Тестирование

		применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6); способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10); способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);	
2-й этап Умения	Уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1); способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2); способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3); способность принимать участие в организации и сопровождении аттестации объекта	Контрольная работа, Коллоквиум, Тестирование

		информатизации по требованиям безопасности информации (ПК-5); способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6); способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10); способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);	
3-й этап Владения навыками	Владеть методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1); способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2); способность администрировать	Контрольная работа, Коллоквиум, Тестирование

		подсистемы информационной безопасности объекта защиты (ПК-3); способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5); способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6); способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10); способность принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);	

Контрольная работа

Содержание работы.

Для локальной сети, согласно вашему варианту, разработать модель угроз и нарушителя безопасности.

1 – й этап. Производится описание базовой системы;

2 – й этап. Определяются уязвимости базовой системы;

3 – й этап. Определяются угрозы для базовой системы;

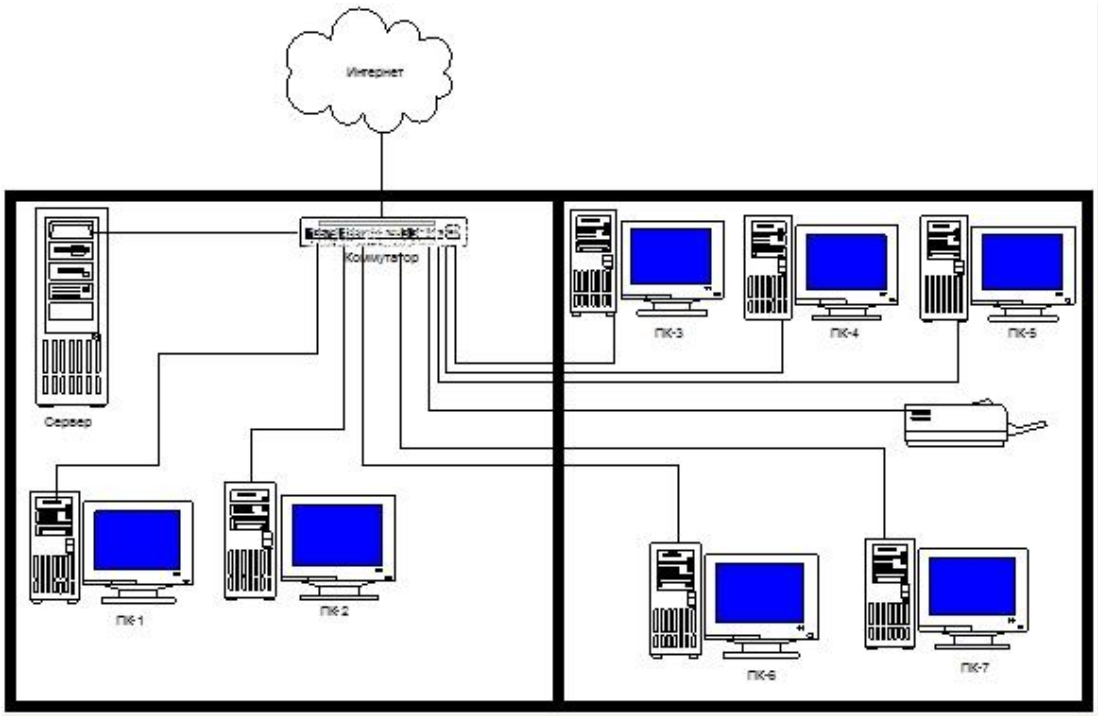
4 – й этап. Определяются нарушители базовой системы;

5 – й этап. Определяется система защиты с набором барьеров;

6 – й этап. Определяется возможные затраты при реализации различных угроз и их комбинаций – строится дерево сценариев.

Вариант 1

ЛВС небольшого торгового предприятия.



Модуль 2. Технология построения защищенных компьютерных систем

Тесты

1В число универсальных сервисов безопасности входят:
1) шифрование
2) средства построения виртуальных частных сетей
3) туннелирование

2Комплексное экранирование может обеспечить:
1) разграничение доступа по сетевым адресам
2) выборочное выполнение команд прикладного протокола
3) контроль объема данных, переданных по TCP-соединению

3Уровень безопасности С, согласно "Оранжевой книге", характеризуется:
1) произвольным управлением доступом
2) принудительным управлением доступом
3) верифицируемой безопасностью

4Перехват данных является угрозой:
1) доступности
2) конфиденциальности
3) целостности

5В число целей политики безопасности верхнего уровня входят:

6 "Общие критерии" содержат следующие виды требований:
1) функциональные
2) доверия безопасности
3) экономической целесообразности

7Совместно с криптографическими сервисами туннелирование может применяться для достижения следующих целей:
1) обеспечение гарантированной полосы пропускания
2) обеспечение высокой доступности сетевых сервисов
3) обеспечение конфиденциальности и целостности передаваемых данных

8Укажите наиболее существенные с точки зрения безопасности особенности современных российских ИС:
1) доминирование платформы Wintel
2) наличие подключения к Internet
3) наличие разнородных сервисов

9Уголовный кодекс РФ не предусматривает наказания за:
1) увлечение компьютерными играми в рабочее время
2) неправомерный доступ к компьютерной информации

1) формулировка административных решений по важнейшим аспектам реализации программы безопасности
2) выбор методов аутентификации пользователей
3) обеспечение базы для соблюдения законов и правил

3) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

10Уголовный кодекс РФ не предусматривает наказания за:
1) неправомерный доступ к компьютерной информации
2) создание, использование и распространение вредоносных программ
3) массовую рассылку незапрошенной рекламной информации

Модуль 2. Технология построения защищенных компьютерных систем
Коллоквиум

Вопросы коллоквиума:
1. Проблема защиты электронной информации.
2. Место программно-математических методов в комплексной системе защиты информации.
3. Классификация угроз безопасности информации и возможные методы зашиты.
4. Резервное копирование данных: суть, устройства для хранения копии, рекомендации по резервному копированию.
5. Способ хранения информации на мандатных носителях.
6. Структура магнитного диска.
7. Алгоритм записи информации на магнитный диск и возможность восстановления удалённых файлов.
8. Операционная система Windows: алгоритмы удаления информации в Корзину и мимо Корзины.
9. Ошибки файловой системы FAT: супь, причины, способы исправления ситуации.
10. Фрагментирование файлов: суть, причины, программы для дефрагментации.
11. Общий обзор программного обеспечения для профилактического обслуживания носителей информации и восстановления данных.
12. Эффектные меры, повышающие шансы восстановления информации на магнитных носителях.
13. Защита локального компьютера паролем включения: суть, алгоритм настройки, способы преодоления защиты.
14. Загрузка локального компьютера с использованием оригинальной дискеты: суть, программный пример, способы преодоления защиты.
15. Защита локального компьютера паролем заставки экрана, суть, алгоритм настройки, способы преодоления защиты.
16. Защита информации скрытием файлов и папок, изменением имени и расширения, атрибутом «только для чтения»: алгоритмы настройки, способы преодоления защиты.
17. MS Office: алгоритмы защиты документов от несанкционированного доступа и использования. Правила задания пароля. Способы преодоления защиты.
18. Особенности строения файлов текстовых процессоров. Алгоритмы уничтожения удалённого и исправленного текста в теле файла текстового процессора.
19. Применение программ-архиваторов для скрытия и защиты файлов. Правила задания пароля. Способы преодоления защиты.
20. Генератор паролей, алгоритмы генерации. Оценка стойкости пароля.

Критерии оценки модульных работ

Структура работы	Критерии оценки	Распределение баллов

Модуль 1. Информационные технологии и их поддержка		
Контрольная работа	**оценка «5»:** работа выполнена в полном объеме и изложена грамотным языком в определенной логической последовательности с точным использованием специализированной терминологии; показано уверенное владение прикладными программами. **оценка «4»:** работа выполнена в полном объеме, но имеет один из недостатков: в работе допущены один-два недочета при освещении основного содержания ответа; нет определенной логической последовательности, неточно используется специализированная терминология; **оценка «3»:** работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.	5/10/15
Модуль 2. Технология построения защищенных компьютерных систем		
Один вопрос коллоквиума (5 вопросов)	Нет ответа / Неполный ответ / Полный ответ	0/0,5/1
Один тестовый вопрос (10 вопросов)	Нет ответа / Неполный ответ / Полный ответ	0/0,5/1

Типовые экзаменационные материалы

Экзаменационные вопросы:

1. Основы безопасности сетевых информационных технологий.
2. IP-сеть организации.
3. Классификация уязвимостей и атак в компьютерных сетях.
4. Защитные механизмы и средства обеспечения безопасности в компьютерных сетях.
5. Базовые принципы сетевого взаимодействия. Модель OSI. Архитектура TCP/IP.
6. Безопасность физического и канального уровней модели OSI.
7. Сетевые анализаторы и «снифферы».
8. Проблемы безопасности протокола разрешения адресов ARP.
9. Безопасность сетевого уровня модели OSI. Меры защиты сетевого уровня.
10. Приведите примеры того, как злоумышленник может воспользоваться информацией из заголовка IP.
11. Протоколы IP и ICMP.
12. Протокол IPSec.Транспортный и туннельный режимы IPSec.
13. Безопасность транспортного уровня модели OSI. Протоколы TCP и UDP. Меры защиты транспортного уровня.
14. Проблемы безопасности протоколов прикладного уровня (Telnet, FTP, HTTP, SMTP).
15. Понятие о моделях безопасности ОС.
16. Варианты решений по обеспечению безопасности сети организации.
17. Применение межсетевых экранов для защиты корпоративных сетей.
18. Место и роль межсетевых экранов в корпоративных сетях. Типовая корпоративная

сеть.

19. Понятие межсетевых экранов. Защитные механизмы, реализуемые межсетевыми экранами.
20. Обзор документов RFC, имеющих отношение к межсетевым экранам, основные термины и определения. Типы межсетевых экранов.
21. Фильтрация пакетов. Параметры фильтрации. Правила фильтрации. Реализация пакетных фильтров.
22. Понятие демилитаризованной зоны.
23. Особенности фильтрации различных типов трафика.
24. Пакетный фильтр на базе ОС Windows.
25. Шлюзы. Трансляция адресов. Типы трансляции.
26. Шлюзы прикладного уровня, варианты конфигурации.
27. Расположение межсетевых экранов в корпоративной сети.
28. Особенности фильтрации служб прикладного уровня DNS, FTP, SMTP.
29. Противодействие сетевым атакам при помощи межсетевых экранов.
30. Интеграция межсетевых экранов с другими средствами защиты.
31. Достоинства и недостатки межсетевых экранов как средств защиты.
32. Место и роль криптографии в обеспечении безопасности компьютерных сетей.
33. Актуальность проблемы безопасности сетевых технологий.
34. Место и роль криптографических методов и средств в системах управления и электронной коммерции.
35. Задачи, решаемые средствами криптографической защиты информации: обеспечение конфиденциальности, целостности и аутентичности данных, разграничение ответственности, аутентификация абонентов.
36. Электронные цифровые подписи. Механизмы цифровой подписи.
37. Техника контроля использования асимметричных ключей.
38. Концепция инфраструктуры открытых ключей (PublicKeyInfrastructure — PKI). Основные термины и определения. Компоненты PKI и их функции: орган сертификации, органы регистрации, владельцы сертификатов, клиенты и клиентское программное обеспечение, хранилище сертификатов.
39. Модели доверия при наличии различных органов сертификации. Цепочки сертификатов и сертификационные пути. Доверие с разделенными доменами.
40. Какие существуют методы оценки защищенности компьютерной сети?
41. Перечислить и описать разновидности биометрических систем идентификации личности.
42. Описать принцип аналитического метода оценки защищенности компьютерной сети.
43. Описать принцип имитационного метода оценки защищенности компьютерной сети.
44. Перечислить основные правила обеспечения политики безопасности информации в компьютерных сетях.
45. Частные и виртуальные частные сети.
46. Классификация VPN.
47. Какие технологии в сетях VPN используются, чтобы обеспечить безопасность в компьютерных сетях?
48. Защита удаленного доступа.
49. Аудит и мониторинг безопасности компьютерных сетей.
50. Стандарты информационной безопасности.

Структура экзаменационного билета.
Экзаменационный билет включает в себя два теоретических вопроса и одну задачу.
Примерные вопросы для экзамена:
1. Теоретический вопрос.
2. Теоретический вопрос.

3. Задача

Образец экзаменационного билета

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Институт истории и государственного управления

Направление 10.03.01 «Информационная безопасность»

Дисциплина Защита информационных процессов в компьютерных системах

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Основы безопасности сетевых информационных технологий.
2. Стандарты информационной безопасности.
3. Нарисовать стандартную модель OSI? Что стандартизует стек OSI?

Зав. кафедрой управления информационной безопасностью А.С. Исмагилова

Кафедра управления информационной безопасностью

Критерии и методика оценивания (в баллах):

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

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

- 10-16 баллов выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос. Студент не решил задачу или при решении допущены грубые ошибки;

- 1-10 баллов выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.

Перевод оценки из 100-балльной в четырех балльную производится следующим образом:

- 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.

Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в приложении 2.

5. Учебно-методическое и информационное обеспечение дисциплины

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

основная учебная литература

1. Спицын В.Г.Информационная безопасность вычислительной техники: учебное пособие. - Томск: Эль Контент, 2011. – 148 с. http://biblioclub.ru/index.php?page=book&id=208694&sr=1
2. Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В.Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов. - М.: Флинта, 2011. – 224 с. http://biblioclub.ru/index.php?page=book&id=93351&sr=1
3. Фефилов А.Д.Методы и средства защиты информации в сетях. - М.: Лаборатория книги, 2011. – 103 с. http://biblioclub.ru/index.php?page=book&id=140796&sr=1

дополнительная учебная литература

4. Гуц А.К., Вахний Т.В.Теория игр и защита компьютерных систем. - Омск: Омский государственный университет, 2013. – 160 с. http://biblioclub.ru/index.php?page=book&id=237190&sr=1
5. Андрончик А.Н., Коллеров А.С., Синадский Н.И., Щербаков М.Ю.Сетевая защита на базе технологий фирмы CiscoSystems. Практический курс: учебное пособие. - Екатеринбург: Издательство Уральского университета, 2014. – 179 с. http://biblioclub.ru/index.php?page=book&id=275694&sr=1
6. Никифоров С.В. Введение в сетевые технологии: Элементы применения и администрирования сетей: учебное пособие. - М.: Финансы и статистика, 2007. – 224 с. http://biblioclub.ru/index.php?page=book&id=221461&sr=1

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. www.fstec.ru –сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России

7. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. 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);
9. www.newlibrary.ru – Новая электронная библиотека;
10. www. edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. 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.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
15. 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	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 лабораторных работ*****:** Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения	Лекции, практические 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 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 МА1225 – 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 МА1225 – 1 шт. **Аудитория № 416**

информационной безопасности № 507 (гуманитарный корпус), лаборатория полигон технической защиты информации № 508 (гуманитарный корпус), компьютерный класс, аудитория 404 (гуманитарный корпус), 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 № 510 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **4.** ***учебная аудитория для проведения групповых и индивидуальных консультаций, учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 510 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610		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. **Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507** Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технические средства обработки информации, стенд "Устройство ПК". **Лаборатория полигон технической защиты информации № 508** Учебная мебель, учебно-наглядные пособия, аудиторная доска трех-секционная, плакаты с тематикой технической защиты информации, комплекс мониторинга WiFi сетей "Зодиак II", универсальный ком-плект инструментов для проведения работ по специальным провер-кам и специальным обследованиям Калейдоскоп-П2, многофункциональный поисковый прибор ST-031M "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон". **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 510** 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**

(гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **5.** ***помещения для самостоятельной работы:*** аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус). **6.** ***помещение для хранения и профилактического обслуживания учебного оборудования:*** аудитория № 523 (гуманитарный корпус).		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. 1. Windows 8 Russian Russian OLP NL AcademicEditionи 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. 3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

Приложение 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины **Защита информационных процессов в компьютерных системах** на 7 семестр

очная форма обучения

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
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 7 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
1.	Информационные технологии	2	2	-	10	Осн: 1-3 Доп: 4-6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников. Выполнение практической работы	Контрольная работа, Коллоквиум, Тестирование
2.	Поддержка информационных технологий	4	4		5	Осн: 1-3 Доп: 4-6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников. Выполнение практической работы	Контрольная работа, Коллоквиум, Тестирование
3.	Основные угрозы безопасности информации информационных	2	2	-	10	Осн: 1, 3 Доп: 4- 6	Самостоятельное изучение рекомендуемой основной и	Контрольная работа, Коллоквиум, Тестирование

	технологиях						дополнительной литературы выполнение рефератов	
4.	Основные угрозы безопасности информации в компьютерных системах	4	4		5	Осн: 1, 3 Доп: 4- 6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы выполнение рефератов	Контрольная работа, Коллоквиум, Тестирование
5.	Государственная политика в области информационной безопасности	2	2	-	5	Осн: 1, 2 Доп: 4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Контрольная работа, Коллоквиум, Тестирование
6.	Государственная политика в области безопасности компьютерных систем	4	4		10	Осн: 1, 2 Доп: 4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, выполнение практической работы	Контрольная работа, Коллоквиум, Тестирование
Всего		18	18	-	45			

Приложение 2

Рейтинг – план дисциплины
Защита информационных процессов в компьютерных системах

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Информационные технологии и их поддержка				
Текущий контроль			**0**	**20**
1. Аудиторная работа	5	1	0	5
2. Контрольная работа	15	1	0	15
Рубежный контроль			**0**	**15**
1.Контрольная работа	15	1	0	15
Модуль 2. Технология построения защищенных компьютерных систем				
Текущий контроль			**0**	**20**
1. Аудиторная работа	7	2	0	14
2. Оформление лабораторных работ	2,5	2	0	5
Рубежный контроль			**0**	**15**
1.Тесты	10	1	0	10
2. Коллоквиум	5	1	0	5
Поощрительные баллы				
1. Студенческая олимпиада	5			5
2. Участие в конференциях	5			5
3. Публикация статей	5			5
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
Посещение лекционных занятий			0	–6
2. Посещение практических (семинарских, лабораторных занятий)			0	–10
Итоговый контроль				
Экзамен			0	30