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

Актуализировано:
на заседании кафедры
протокол № 10 от «7» июня 2018 г.
Зав. кафедрой / А.С. Исмагилова

Согласовано:
Председатель УМК института
/ Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информационных процессов в компьютерных системах

Б1.Б.31.03 (базовая)

Программа специалитета

Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация
Технологии защиты информации в правоохранительной сфере

Квалификация
Специалист по защите информации

Разработчики (составители)
Ст.преподаватель,
канд.физ.-мат.наук / Ахмеров А.А.

Ассистент / Фатхелисламов А.Ф.

Для приема: 2015 г.

Уфа 2018 г.

Составитель / составители: А.А. Ахмеров, А.Ф. Фатхелисламов

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью протокол №_10_от «_23_»__июня___20_18_ 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/

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. 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 к деловому общению, профессиональной коммуникации на одном из иностранных языков. (ОПК-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 исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПСК-3)	

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;	способность к деловому общению, профессиональной коммуникации на одном из иностранных языков. (ОПК-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 исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПСК-3)	
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 к деловому общению, профессиональной коммуникации на одном из иностранных языков. (ОПК-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	

	учетом установленных требований;	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 исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПСК-3)	

2. **Цель и место дисциплины 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

Эти дисциплины направлены на формирование компетенций ОК-1, ПК-2, ПК-3, ПК-5, ПК-6, ПСК-3.

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

ОК-11: способность к деловому общению, профессиональной коммуникации на одном из иностранных языков

Этап	Планируемые	Критерии оценивания результатов обучения	
(уровень) освоения компетенции	результаты обучения (показатели достижения заданного уровня освоения компетенций)	Не зачтено	Зачтено
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 информационной безопасности; типы	Не знает	Демонстрирует целостность знания об об аппаратных средствах вычислительной техники; операционных системх персональных ЭВМ; основах администрирования вычислительных сетей; системах управления БД; эксплуатационных и технико-экономических характеристиках программных и технических средств защиты информации и обеспечения информационной безопасности; типах технических и программно-аппаратных средств обработки и защиты информации

	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 установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	Не умеет	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: методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации	Не владеет	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	
		Не зачтено	Зачтено
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	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	Не умеет	Уверенно использует существующие пакеты прикладных программ для решения поставленной задачи; реализует и

	программ для решения поставленной задачи; реализовать и отлаживать пакеты прикладных программ; решать задачи проектирования программных систем с помощью различных методов		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

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	
		Не зачтено	Зачтено

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 программным обеспечением; характеристики аппаратных средств борьбы с утечкой информации.	Не знает	Демонстрирует целостность знания об методах и средствах управления защитой информации в операционных системах, базах данных и прикладных программах; настройке и конфигурировании 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	Не умеет	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

	на применение технические средства защиты данных		
Третий этап (уровень)	Владеть: навыками анализа и оценки угроз информационной безопасности объекта	Не владеет	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	
		Не зачтено	Зачтено
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;	Не знает	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 анализу структур; общеметодологических принципах теории информационной безопасности; возможностях и особенностях организационных, аппаратных и программных средств безопасности и защиты информации; состоянии законодательной

	общеметодологические принципы 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;		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; использовать закономерности преобразования данных в каналах при	Не умеет	Сформированное умение применять принципы политики безопасности; закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности; обосновывать организационно-технические мероприятия по защите информации; использовать

	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.		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, практические приемы и пр.) для управления информационной безопасностью; навыками организации комплекса мероприятий по защите информации в	Не владеет	Сформированное владение навыками анализа, обработки и интерпретации результатов решения прикладных задач 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

	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.		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	
		Не зачтено	Зачтено

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	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 документацио	Не умеет	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

	нной 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 проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	Не владеет	Владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации; методами сбора и анализа исходных 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	Планируемые результаты обучения	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено

компетенции	(показатели достижения заданного уровня освоения компетенций)		
Первый этап (уровень)	Знать: основные принципы оценки работоспособности и тестирования оборудования обработки и передачи данных; критерии и меры надежности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	Не знает	Демонстрирует целостность знания об основных принципах оценки работоспособности и тестирования оборудования обработки и передачи данных; критерии и меры надежности, 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	Не умеет	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.

	атаки, нарушающие систему информационной безопасности.		
Третий этап (уровень)	Владеть: навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; использования методов тестирования коммуникационного оборудования и аппаратуры обработки данных, криптографических систем	Не владеет	Владеет навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий; использования методов тестирования коммуникационного оборудования и аппаратуры обработки данных, криптографических систем

ПСК-3: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать: критерии оценки уровня информационной безопасности объектов и	Не знает	Демонстрирует целостность знаний критериев оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов

	систем с использованием отечественных стандартов		
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 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 нормативных документов; навыками анализа и интерпретации информации, содержащейся	Не владеет	Владеет методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; обладает навыками анализа и интерпретации информации, содержащейся в различных источниках

	в различных источниках		

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).

Шкала оцениваниядля зачета:

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

не зачтено – от 0 до 59 рейтинговых баллов).

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 к деловому общению, профессиональной коммуникации на одном из иностранных языков. (ОПК-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	Аудиторная работа (допуски к лабораторным работам), контрольная работа, оформление лабораторных работ, тестирование, коллоквиум

		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 исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПСК-3)	
2-й этап Умения	Уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	способность к деловому общению, профессиональной коммуникации на одном из иностранных языков. (ОПК-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	Аудиторная работа (допуски к лабораторным работам), контрольная работа, оформление лабораторных работ, тестирование, коллоквиум

		работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6); способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПСК-3)	
3-й этап Владения навыками	Владеть методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации	способность к деловому общению, профессиональной коммуникации на одном из иностранных языков. (ОПК-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	Аудиторная работа (допуски к лабораторным работам), контрольная работа, оформление лабораторных работ, тестирование, коллоквиум

		эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6); способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПСК-3)	

Для оценивания результатов обучения в виде знаний используются следующие типы контроля:

- индивидуальный и групповой опрос;
- тестирование,
- письменные ответы на вопросы.

I - простые, II - комплексные вопросы; знать – «3»

Примерные вопросы для проверки знаний по компетенции ОК-11:

ПК-1 – I.З

Перечислить и дать общую характеристику основных стандартных подходов защиты компьютерных сетей.

ПК-1 – II.З

Перечислить и дать общую характеристику основных нестандартных подходов защиты компьютерных сетей.

Примерные вопросы для проверки знаний по компетенции ПК-2:

ПК-2 – I.З

Назначение электронного замка "Соболь". Состав, реализуемые функции и возможности. Принципы работы и варианты применения.

ПК-2 – II.З

Механизмы защиты Secret Net

Примерные вопросы для проверки знаний по компетенции ПК-3:

ПК-3 – I.З

Предсказуемое расположение ресурсов.

ПК-3 – II.З

Анализ содержимого почтового и Web-трафика (Content Security). Системы анализа содержимого.

Примерные вопросы для проверки знаний по компетенции ПК-4:

ПК-4 – I.З

Перечислить и дать общую характеристику основных программно-аппаратных средств защиты компьютерных сетей.

ПК-4 – II.З
Перечислить и дать общую характеристику основных элементов современных криптографических средств компьютерных сетей.

Примерные вопросы для проверки знаний по компетенции ПК-5:
ПК-5 – I.З
Защита информации в компьютерных сетях. Объекты защиты информации в сети.
ПК-5 – II.З
Методы защиты информации от преднамеренного доступа в компьютерных сетях.

Примерные вопросы для проверки знаний по компетенции ПК-6:
ПК-6 – I.З
Сетевое оборудование.
ПК-6 – II.З
Виды межсетевых экранов.

Примерные вопросы для проверки знаний по компетенции ПСК-3:
ПК-10 – I.З
Основные возможности межсетевых экранов.
ПК-10 – II.З
Применение виртуальных частных сетей.

Для оценивания результатов обучения в виде умений и владений используются практические контрольные задания (ПКЗ), включающих одну или несколько задач (вопросов) в виде краткой формулировки действий (комплекса действий), которые следует выполнить, или описание результата, который нужно получить.

По сложности ПКЗ разделяются на простые и комплексные задания.

Простые ПКЗ предполагают решение в одно или два действия. К ним можно отнести: простые ситуационные задачи с коротким ответом или простым действием; несложные задания по выполнению конкретных действий. Простые задания применяются для оценки умений.

Комплексные задания требуют многоходовых решений как в типичной, так и в нестандартной ситуациях. Это задания в открытой форме, требующие поэтапного решения и развернутого ответа, в т.ч. задания на индивидуальное или коллективное выполнение проектов, на выполнение практических действий или лабораторных работ. Комплексные практические задания применяются для оценки владений.

Примерные формулировки практических контрольных заданий

I - простые, II - комплексные задания;. уметь – «У» / владеть – «В»

Примерные вопросы для проверки знаний по компетенции ОК-11:
ПК-1 – I.У
Создание перечня систем идентификации и аутентификации на индивидуальном предприятии. Аудит журналов брандмауэра
ПК-1 – II.У
Перечислить и дать общую характеристику основных количественных и качественных метрик, используемых в области информационной безопасности.

ПК-1 – I.В
Обнаружение сетевых атак.
ПК-1 – II.В
Методы контроля за исполнением должностных инструкций. Методы и формы организационной защиты информации. Методы организационной защиты информации. Виды перекрытия каналов утечки информации

Примерные вопросы для проверки знаний по компетенции ПК-2:
ПК-2 – I.У
С помощью антивирусной программы провести проверку программы на наличие вирусов.
ПК-2 – II.У
Установить и настроить межсетевой экран.

ПК-2 – I.В
Управление доступом к информации. Защита компьютерных систем от вредоносного программного воздействия
ПК-2 – II.В
Шлюзы уровня соединения. Реализация трансляции адресов в ОС Linux. Реализация трансляции адресов в ОС Windows.

Примерные вопросы для проверки знаний по компетенции ПК-3:
ПК-3 – I.У
Проводить анализ основных количественных и качественных метрик, используемых в области информационной безопасности.
ПК-3 – II.У
Описание форм представления данных в компьютерных системах.

ПК-3 – I.В
Оценка политик безопасности
ПК-3 – II.В
Определение уровня исходной защищенности информации.

Примерные вопросы для проверки знаний по компетенции ПК-4:
ПК-4 – I.У
Определение периметра IP-сети организации.
ПК-4 – II.У
Применение программных средств аудита информационной безопасности с целью тестирования состояния защищенности компьютерных систем от несанкционированного доступа и выработки мер защиты от выявленных угроз

ПК-4 – I.В
Модели безопасного взаимодействия в КС. Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды
ПК-4 – II.В
Меры защиты от атак на протокол ARP, утилита arpwatch. Обнаружение сетевых анализаторов с помощью протокола ARP, утилита Cain.

Примерные вопросы для проверки знаний по компетенции ПК-5:
ПК-5 – I.У
Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов.

ПК-5 – II.У
С помощью программы восстановления системы исправить ошибки системного реестра.

ПК-5 – I.В
Составление должностной инструкции
ПК-5 – II.В
Произвести технический, экономический и организационный анализ показателей применимости программного обеспечения компьютерной сети.

Примерные вопросы для проверки знаний по компетенции ПК-6:
ПК-6 – I.У
Установка и конфигурирование сетевых адаптеров.
ПК-6 – II.У
Установка и конфигурация сетевого оборудования для объединения сетей

ПК-6 – I.В
Работа с системой управления коммутатором
ПК-6 – II.В
Настройка маршрутизаторов для удаленного доступа.

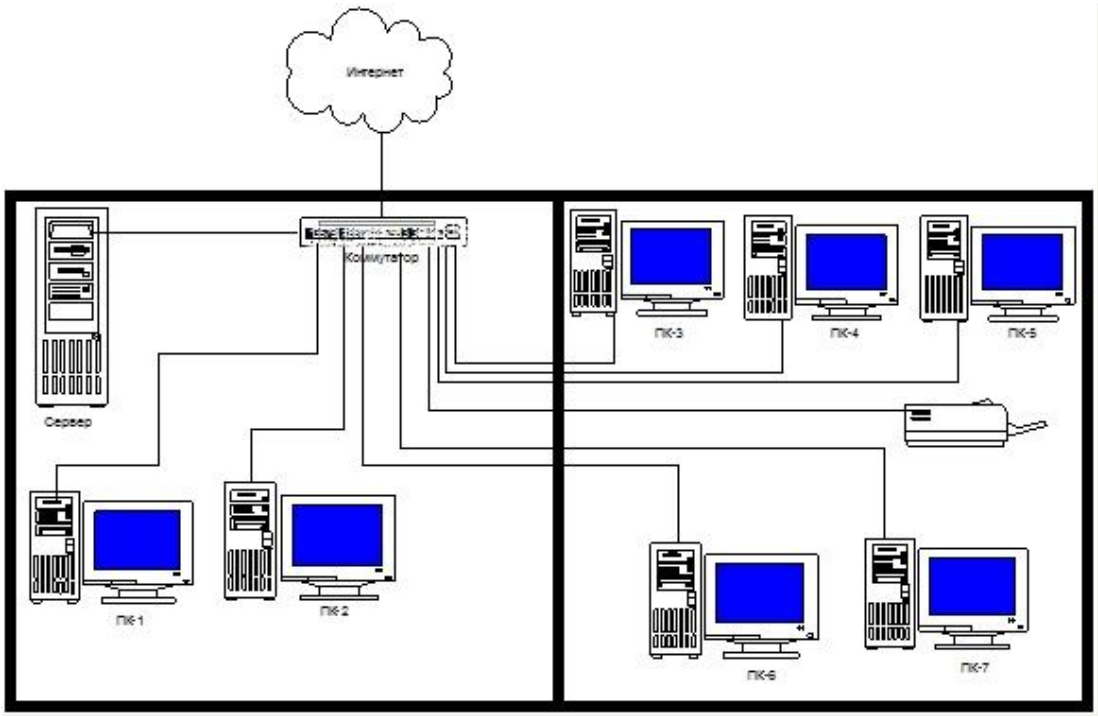
Примерные вопросы для проверки знаний по компетенции ПСК-3:
ПК-10 – I.У
Установка клиентского и серверного системного программного обеспечения
ПК-10 – II.У
Диагностирование сетевых протоколов TCP/IP

ПК-10 – I.В
Структурирование локальных сетей
ПК-10 – II.В
Установка и удаление сетевых служб

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

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
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.		
КСР	**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.		
Один вопрос коллоквиума (5 вопросов)	Нет ответа / Неполный ответ / Полный ответ	0/0,5/1
Один тестовый вопрос (15 вопросов)	Нет ответа / Неполный ответ / Полный ответ	0/0,5/1

Типовые вопросы к зачету

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.

5.3 Рейтинг-план дисциплины (при необходимости)

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

а)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

б)дополнительная учебная литература:

1. 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
2. Заика А.Компьютерная безопасность. - М.: Рипол Классик, 2013. – 160 с.
http://biblioclub.ru/index.php?page=book&id=227317&sr=1
3. 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
4. Характеристика и особенности локальных компьютерных сетей. - М.: Лаборатория книги, 2012. – 157 с.
http://biblioclub.ru/index.php?page=book&id=142934&sr=1
5. 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
6. Павлюк В.Д. Типовые топологии вычислительных сетей. - М.: Лаборатория книги, 2011. – 105 с.
http://biblioclub.ru/index.php?page=book&id=142528&sr=1

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

- Электронная библиотечная система БашГУ – www.bashlib.ru
- Электронная библиотечная система «ЭБ БашГУ» - https://elib.bashedu.ru/
- Электронная библиотечная система «Университетская библиотека онлайн» - https://biblioclub.ru/
- Электронная библиотечная система издательства «Лань» - https://e.lanbook.com/
- Электронный каталог Библиотеки БашГУ - http://www.bashlib.ru/catalogi/

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:*** компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс	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 AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **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

аудитория № 420 (гуманитарный корпус). **3.** ***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). **4.** ***учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **5.** ***помещения для самостоятельной работы:*** читальный зал библиотеки аудитория		АРАРТ МА1225 – 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 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. 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. 3. Система централизованного тестирования БашГУ (Moodle). GNU General Public License.

402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **6. *помещение для хранения и профилактического обслуживания учебного оборудования:***аудитория № 523 (гуманитарный корпус).		

Приложение 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины **Защита информационных процессов в компьютерных системах** на 6 семестре

очная форма обучения

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	5 ЗЕТ / 180 часов
Учебных часов на контактную работу с преподавателем:	80
лекций	32
практических / семинарских	48
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	-
Учебных часов на самостоятельную работу обучающихся, включая подготовку к экзамену / зачету	100

Форма контроля
Зачет 6 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 и их поддержка	12	12	6	40	Осн: 1-3 Доп: 1-6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников. Выполнение практической работы	Контрольная работа
2.	Основные угрозы безопасности информации в компьютерных системах	10	10	5	30	Осн: 1, 3 Доп: 1- 3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы выполнение рефератов	Тесты
3.	Государственная политика в области безопасности	10	10	5	30	Осн: 1, 2 Доп: 3	Самостоятельное изучение рекомендуемой основной и	Коллоквиум

	компьютерных систем						дополнительной литературы, выполнение практической работы	
	Всего часов	32	32	16	100			

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. Архитектура информационных сетей. Основные понятия и определения				
Текущий контроль			**0**	**26**
1. Аудиторная работа (допуски к лабораторным работам)	3	8	0	24
2. Домашние задания (оформление лабораторных работ)	1	2	0	2
Рубежный контроль			**0**	**25**
1.Тесты	25	1	0	25
Модуль 2. Тенденции развития телекоммуникационных систем и сетей				
Текущий контроль			**0**	**24**
1. Аудиторная работа (допуски к лабораторным работам)	2	8	0	16
2. Домашние задания (оформление лабораторных работ)	1	8	0	8
Рубежный контроль			**0**	**25**
1.Контрольная работа	25	1	0	25
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				
Зачет			0	00