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 информации в компьютерных сетях

(Б1.В.1.ДВ.09.02 дисциплина по выбору)

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):
Старший преподаватель,
канд.хим.наук / А.А.Султанова

Старший преподаватель / А.М. Махмутов

Для приема: 2014 г.

Уфа 2018 г.

Составители: А.А.Султанова, А.М.Махмутов

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью протокол №10 от «7» июня 2018 г.

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

Заведующий кафедрой ___________________/ _____________Ф.И.О/

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

Заведующий кафедрой ___________________/ _____________Ф.И.О/

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

Заведующий кафедрой ___________________/ _____________Ф.И.О/

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

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

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

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	1. общенаучные методы и понятия, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	– способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач (ОПК-1)	
	2. политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, 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	– способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК-1)	
	3. аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД, эксплуатационные и технико-экономические	– способность применять технические и программно-аппаратные средства обработки и защиты информации (ПК-2)	

	характеристики программных и технических средств защиты информации и обеспечения информационной безопасности, типы технических и программно-аппаратных средств обработки и защиты информации, основные направления политик защиты информации на предприятии (организации)		
	4. политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	– способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации (ПК-3)	
	5. аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД; эксплуатационные и технико-экономические характеристики технических средств защиты информации и обеспечения информационной безопасности; типы технических средств обработки и защиты информации; основные направления политик защиты информации на предприятии (организации)	– способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния (ПК-5)	

	6. особенности защиты государственной тайны, состояние законодательной базы и стандарты в области защиты государственной тайны	– способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации (ПК-30)	
Умения	1. моделировать и прогнозировать развитие процессов и явлений при решении профессиональных задач с использованием общенаучных методов и понятий, законов физики, математического аппарата	– способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач (ОПК-1)	
	2. реализовывать на практике 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	– способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК-1)	
	3. формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, осуществлять меры противодействия нарушениям сетевой	– способность применять технические и программно-аппаратные средства обработки и защиты информации (ПК-2)	

	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		
	4. реализовывать на практике принципы политики безопасности, использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	– способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации (ПК-3)	
	5. 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 аппаратных средств защиты информации, выполнять работы по установке, конфигурированию и эксплуатации компонентов технических систем обеспечения информационной	– способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния (ПК-5)	

	безопасности и защиты информации		
	6. обосновывать организационно-технические мероприятия по защите государственной тайны, ориентироваться в нормативно-правовых актах, регламентирующих сферу защиты государственной тайны, планировать внедрение и внедрять компоненты систем предприятия, обеспечивающих безопасность государственной тайны	– способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации (ПК-30)	
Владения (навыки / опыт деятельности)	1. использования методов моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	– способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач (ОПК-1)	
	2. 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	– способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК-1)	

	электронного оборудования и информационно-коммуникационных технологий, навыками внедрения, адаптации и настройки средств защиты прикладных ИС		
	3. оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации	– способность применять технические и программно-аппаратные средства обработки и защиты информации (ПК-2)	
	4. 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	– способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации (ПК-3)	
	5. оценки, тестирования. настройки и применения компонентов технических систем обеспечения защиты информации	– способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния (ПК-5)	
	6. обоснования, выбора, реализации и контроля результатов управленческого решения, выявления и устранения угроз информационной безопасности, эксплуатации современного электронного оборудования и информационно-	– способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации (ПК-30)	

	коммуникационных технологий, внедрения, адаптации и настройки средств защиты прикладных ИС		

2. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации в компьютерных сетях» относится к дисциплинам вариативной части образовательной программы.

Дисциплина изучается на 5 курсе в 9 семестре.

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

Изучение дисциплины базируется на знаниях, умениях и навыках, сформированных в результате освоения студентами предшествующих дисциплин образовательной программы по направлению подготовки 10.05.05 – «Безопасность информационных технологий в правоохранительной сфере» профиля «Технологии защиты информации в правоохранительной сфере»: «Физика», «Информатика».

Эта дисциплина направлена на формирование компетенций ОПК-1, ПК-1, ПК-2, ПК-3, ПК-5, ПК-30.

Освоение дисциплины «Защита информации в компьютерных сетях» служит основой для выполнения практических мероприятий по защите информации. Полученные знания, навыки и умения используются при прохождении преддипломной практики и в ходе выполнения выпускной квалификационной работы.

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

Содержание рабочей программы представлено в Приложении 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

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

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать: основные понятия и задачи в области информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности	Имеет фрагментарные знания об основных понятиях в области общенаучных методов, понятия, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	Демонстрирует целостность знания об основных понятиях и задачах в области информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности
Второй этап (уровень)	Уметь: работать с офисными программами, проводить поиск информации, осуществлять сбор и анализ данных, необходимых для проведения конкретных расчетов;	Умеет работать и смоделировать, прогнозировать развитие процессов и явлений при решении профессиональных задач с использованием общенаучных	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.	методов и понятий, законов физики, математического аппарата	обрабатывать массивы данных в соответствии с поставленной задачей.
Третий этап (уровень)	Владеть: информационно-коммуникационными технологиями с учетом основных требований информационной безопасности.	Не способен выбрать необходимые для работы информационно-коммуникационные технологии.	Владеет способностью выбора и использования информационно-коммуникационными технологиями с учетом основных требований информационной безопасности.

ПК-1. Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.

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	Имеет фрагментарные знания о законодательной базе обеспечения информационной безопасности	Знает основные законодательные акты по защите информации в государственных и частных структурах
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 показывает сформированные умения опираться на законодательную базу, а также разрабатывать организационно-распорядительные документы по защите информации	Аргументировано обосновывать и представлять необходимость применения конкретного типа средств противодействия перехвату электронных документов; Уметь применять методы защищенной автоматизации обработки документов
Третий этап (уровень)	Владеть: Навыками работы с нормативными 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	Отсутствуют навыки работы с нормативными правовыми актами и навыками лицензирования в области защиты информации;	Владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации; может спроектировать систему защиты информации,

ПК-2. Способность применять технические и программно-аппаратные средства обработки и защиты 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: виды и формы информации, подверженной угрозам; средства защиты от несанкционированного доступа; средства для обнаружения атак и анализа защищенности объекта	Имеет фрагментарные знания об основных видах и формах информации и средств для ее анализа и защиты	Знает основные виды и формы информации и средства для ее анализа и защиты
Второй этап (уровень)	Уметь: использовать возможности информационных систем для обеспечения информационной безопасности предприятия; работать с ПК, как со средством защиты информации	Не показывает сформированные умения в использовании возможностей информационных систем и в работе с ПК, как со средством защиты информации	Уверенно использует возможности информационных систем для обеспечения информационной безопасности предприятия и работает с ПК, как со средством защиты информации
Третий этап (уровень)	Владеть: методикой определения видов информации; навыками анализа угроз информационно-вычислительным системам и путей их реализации	Не способен определять виды информации, анализировать угрозы информационно-вычислительным системам	Владеет методикой определения видов информации; навыками анализа угроз информационно-вычислительным системам и путей их реализации

ПК-3. Способность организовывать и проводить мероприятия по контролю за

обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты 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: подходы обоснования затрат на информационную безопасность; методы и модели установления зависимости между затратами на защиту информации и уровнем защищенности, нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом; стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов; методики анализа рисков информационных систем	Фрагментарные представления о подходах к обоснованию затрат на информационную безопасность, Имеет фрагментарные знания о нормативно-правовых документах по обеспечению информационной безопасности в нашей стране и за рубежом; стандартах построения систем информационной безопасности и стандартах оценки степени защиты систем информационной безопасности объектов; методиках анализа рисков информационных систем	Сформированные представления о подходах к обоснованию затрат на информационную безопасность; методах и моделях установления зависимости между затратами на защиту информации и уровнем защищенности, свободное знание нормативно-правовые документов по обеспечению информационной безопасности в нашей стране и за рубежом; стандартов построения систем информационной безопасности и стандартов оценки степени защиты систем информационной безопасности объектов; методик анализа рисков информационных систем
Второй этап (уровень)	Уметь: оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; самостоятельно находить нужную информацию по тематике и выбирать необходимые для организации информационные ресурсы и источники знаний в электронной среде; использовать основные методики оценки совокупной стоимости владения для подсистемы информационной безопасности; определять зависимость между затратами на ИБ и уровнем защищенности, интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных, разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	Слабо выраженные способности к работе с данными, использованию основных методик оценки совокупной стоимости владения для подсистемы информационной безопасности; определению зависимости между затратами на ИБ и уровнем защищенности; слабые умения интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных, разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	Умеет оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; самостоятельно находить нужную информацию; использовать основные методики оценки совокупной стоимости владения для подсистемы информационной безопасности; определять зависимость между затратами на ИБ и уровнем защищенности, способен уверенно интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных, разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества
Третий этап (уровень)	Владеть: навыками определения затрат компании на ИБ, навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений, методологией и навыками решения научных и практических задач	Фрагментарные навыки определения затрат компании на ИБ, слабые навыки интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений, методологией и навыками решения научных и практических задач	Успешное и систематическое применение навыков определения затрат компании на ИБ, уверенные навыки интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений, методологией и навыками решения научных и практических задач

ПК-5. Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)		
		Не зачтено	Зачтено
Первый этап (уровень)	Знать: критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов	Имеет фрагментарные знания о критериях оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов	Демонстрирует целостность знаний критериев оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов
Второй этап (уровень)	Уметь: Применять отечественные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; собирать, анализировать и интерпретировать	Умеет использовать отечественные стандарты в области компьютерной безопасности, но не способен применить их для проектирования, разработки и оценки защищенности компьютерных систем; не способен	Умеет эффективно применять отечественные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; собирать,

	необходимую информацию, содержащуюся в различных формах отчетности и прочих источниках	собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих источниках	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 в различных источниках	Не способен провести проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.	Владеет методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; обладает навыками анализа и интерпретации информации, содержащейся в различных источниках

ПК-30. Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать: особенности защиты государственной тайны, состояние законодательной базы и стандарты в области защиты государственной тайны	Имеет фрагментарные знания об особенностях защиты государственной тайны, состояние законодательной базы и стандарты в области защиты государственной тайны	Демонстрирует целостность знаний особенностей защиты государственной тайны, состояние законодательной базы и стандарты в области защиты государственной тайны
Второй этап (уровень)	Уметь: обосновывать организационно-технические мероприятия по защите государственной тайны, ориентироваться в нормативно-правовых актах, регламентирующих сферу защиты государственной тайны, планировать внедрение и внедрять компоненты систем предприятия, обеспечивающих безопасность государственной тайны	Не умеет обосновывать организационно-технические мероприятия по защите государственной тайны, ориентироваться в нормативно-правовых актах, регламентирующих сферу защиты государственной тайны, планировать внедрение и внедрять компоненты систем предприятия, обеспечивающих безопасность государственной тайны	Умеет эффективно обосновывать организационно-технические мероприятия по защите государственной тайны, ориентироваться в нормативно-правовых актах, регламентирующих сферу защиты государственной тайны, планировать внедрение и внедрять компоненты систем предприятия, обеспечивающих безопасность государственной тайны
Третий этап (уровень)	Владеть: обоснования, выбора, реализации и контроля результатов управленческого решения, выявления и устранения угроз информационной безопасности, эксплуатации современного электронного оборудования и информационно-коммуникационных технологий, внедрения, адаптации и настройки средств защиты прикладных ИС	Не способен обосновать выбор, реализации и контроля результатов управленческого решения, выявления и устранения угроз информационной безопасности, эксплуатации современного электронного оборудования и информационно-коммуникационных технологий, внедрения, адаптации и настройки средств защиты прикладных ИС	Владеет методиками обоснования, выбора, реализации и контроля результатов управленческого решения, выявления и устранения угроз информационной безопасности, эксплуатации современного электронного оборудования и информационно-коммуникационных технологий, внедрения, адаптации и настройки средств защиты прикладных ИС

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей дисциплины, перечисленных в рейтинг-плане дисциплины, для зачета: текущий контроль – максимум 30 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10.

Шкала оценивания для 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	общенаучных методов и понятий, законв физики, математический	ОПК-1: Способность выявлять естественнонаучную	Лабораторная работа, практическая работа, тест, контрольная

	аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач.	работа
	политик, стратегий и технологий информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности, возможностей и особенностей организационных, аппаратных и программных средств безопасности и защиты информации, состояния законодательной базы и стандарты в области информационной безопасности	ПК-1: Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	Лабораторная работа, практическая работа, тест, контрольная работа
	аппаратных средств вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД, эксплуатационных и технико-экономических характеристик программных и технических средств защиты информации и обеспечения информационной	ПК-2: Способность применять технические и программно-аппаратные средства обработки и защиты информации	Лабораторная работа, практическая работа, тест, контрольная работа

	безопасности, типов технических и программно-аппаратных средств обработки и защиты информации, основных направлений политик защиты информации на предприятии (организации)		
	политик, стратегий и технологий информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	ПК-3: Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации	Лабораторная работа, практическая работа, тест, контрольная работа
	аппаратных средств вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД; эксплуатационные и технико-экономические характеристики технических средств защиты информации и обеспечения информационной безопасности; типы технических средств обработки и защиты информации; основные направления политик защиты информации на предприятии (организации)	ПК-5: Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния	Лабораторная работа, практическая работа, тест, контрольная работа
	особенности защиты государственной тайны, состояние законодательной базы и стандарты в области	ПК-30. способность планировать проведение работ по комплексной защите информации и сведений, составляющих	Лабораторная работа, практическая работа, тест, контрольная работа

	защиты государственной тайны	государственную тайну, на объекте информатизации	
2-й этап Умения	моделировать и прогнозировать развитие процессов и явлений при решении профессиональных задач с использованием общенаучных методов и понятий, законов физики, математического аппарата	ОПК-1: Способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач.	Лабораторная работа, практическая работа, тест, контрольная работа
	реализовывать на практике 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	ПК-1: Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	Лабораторная работа, практическая работа, тест, контрольная работа
	формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе,	ПК-2: Способность применять технические и программно-аппаратные средства обработки и защиты информации	Лабораторная работа, практическая работа, тест, контрольная работа

	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		
	реализовывать на практике принципы политики безопасности, использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	ПК-3: Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации	Лабораторная работа, практическая работа, тест, контрольная работа
	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 аппаратных средств защиты информации, выполнять работы по установке, конфигурированию и эксплуатации	ПК-5: Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния	Лабораторная работа, практическая работа, тест, контрольная работа

	компонентов технических систем обеспечения информационной безопасности и защиты информации		
	обосновывать организационно-технические мероприятия по защите государственной тайны, ориентироваться в нормативно-правовых актах, регламентирующих сферу защиты государственной тайны, планировать внедрение и внедрять компоненты систем предприятия, обеспечивающих безопасность государственной тайны	ПК-30. способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации	Лабораторная работа, практическая работа, тест, контрольная работа
3-й этап Владения навыками	навыками использования методов моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	ОПК-1: Способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач.	Лабораторная работа, практическая работа, тест, контрольная работа
	навыками анализа, обработки и интерпретации результатов решения прикладных задач управления, навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной	ПК-1: Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с	Лабораторная работа, практическая работа, тест, контрольная работа

	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 внедрения, адаптации и настройки средств защиты прикладных ИС	учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	
	методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации	ПК-2: Способность применять технические и программно-аппаратные средства обработки и защиты информации	Лабораторная работа, практическая работа, тест, контрольная работа
	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	ПК-3: Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации	Лабораторная работа, практическая работа, тест, контрольная работа

	обработки информации		
	методами оценки, тестирования. настройки и применения компонентов технических систем обеспечения защиты информации	ПК-5: Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния	Лабораторная работа, практическая работа, тест, контрольная работа
	обоснования, выбора, реализации и контроля результатов управленческого решения, выявления и устранения угроз информационной безопасности, эксплуатации современного электронного оборудования и информационно-коммуникационных технологий, внедрения, адаптации и настройки средств защиты прикладных ИС	ПК-30. способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации	Лабораторная работа, практическая работа, тест, контрольная работа

Лабораторная работа

Цель проведения лабораторных работы – практическое освоение материала дисциплины.

Модуль 1, 2

1. Определите настройки протокола TCP/IP вашего компьютера, например, командой ipconfig из командной строки.

2. Установите и запустите средство анализа сетевого трафика. Осуществите захват сетевого трафика.

3. Выполните команду ping *.*.*.* для обнаружения в сети соседнего компьютера.

4. Осуществите просмотр трафика. В полученных сетевых пакетах убедитесь в наличии полей «источник», «приемник», «тип протокола».

5. Найдите пакет, источником которого является Ваш компьютер, тип протокола — ICMP, описание — Echo. Откройте подробное описание данного пакета. Найдите тип пакета и отправляемые данные. Сколько и каких символов отправляется на искомый компьютер?

6. Найдите ответный пакет (приемник — ваш компьютер, тип протокола — ICMP, описание — Echo Reply). Откройте подробное описание данного пакета. Сколько и каких символов отправляется в ответ?

7. Сколько раз осуществляется обмен ICMP-пакетами? Как представлены в IP-пакетах IP-адреса приемника и источника?

Критерии оценки лабораторных работ:

Структура работы	Критерии оценки	Распределение баллов
Одно задание	Нет ответа / Неполный ответ / Полный ответ	0/5/10

Тестирование

Модуль 1

1. К принципам обеспечения безопасности относится:
а) согласованность;
б) взаимная ответственность личности, общества и государства;
в) децентрализации и демократизм.
2. Совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства:
а) угроза информационной безопасности;
б) предполагаемые действия иностранных государств;
в) деятельность иностранных разведок.
3. Не являются видами угроз информационной безопасности:
а) внутренние угрозы;
б) внешние угрозы;
в) значительные угрозы.
4. Не являются видами угроз информационной безопасности:
а) угрозы военные;
б) угрозы потенциальные;
в) угрозы реальные.
5. К методам обеспечения информационной безопасности Российской Федерации относятся:
а) правовые;
б) неправовые;
в) легальные.

Критерии оценки:

Структура работы	Критерии оценки	Распределение баллов
Один вопрос (10 вопрос)	Не правильный ответа / правильный ответ	0/1

Типовые задания для контрольной работы

Модуль 2

Цель проведения контрольной работы – оценка уровня владения базовой профессиональной терминологией. Контрольная работа проводится в письменной форме.

Примеры заданий

1. Альтернативные архитектуры КС.
2. Архитектура сетей Novell.
3. Архитектура DNA.
4. Архитектура AppleTalk.

Критерии оценки контрольных работ:

Структура работы	Критерии оценки	Распределение баллов
Одно задание	Нет ответа / Неполный ответ / Полный ответ	0/5/10

Практическая работа

Модуль 1, 2

Выполняется по результатам изучения темы дисциплины с целью дополнения практического материала (проводится в виде дискуссии).

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

Критерии оценивания:

Структура работы	Критерии оценки	Распределение баллов
Одна тема	Нет ответа / участник дискуссии / подготовка доклада (презентации)	0/5/10

Типовые материалы к зачету

1. Альтернативные архитектуры КС. Архитектура сетей Novell.
2. Альтернативные архитектуры КС. Архитектура DNA.
3. Альтернативные архитектуры КС. Архитектура AppleTalk.
4. Недостатки протокола IPv4. Семейство протоколов IPv6. Основные особенности.
5. Протокол IPv6. Адресация в сетях IPv6.
6. Семейство протоколов IPv6. Сетевой уровень.
7. Семейство протоколов IPv6. Маршрутизация, DNS, транспортные механизмы IPv6.
8. Безопасность в IPv6. Способы совместного сосуществования сетей IPv4 и IPv6. Механизмы перехода на IPv6.
9. Конфигурирование компьютерных сетей. Протоколы RARP, BOOTP, DHCP. Утилиты контроля и диагностики.
10. Управление учетом использования ресурсов. Управление неисправностями. Сетевые анализаторы.
11. Управление доставкой. Доступ к ресурсам с помощью серверов-посредников. Шлюзы уровня приложения (ALG).
12. Управление доставкой. Протокол SOCKS.
13. Управление доставкой. Технология трансляции адресов (NAT). Прозрачные серверыпосредники (transparent proxy).
14. Туннелирование
15. Управление в компьютерных сетях. Модель систем управления ISO. Архитектуры систем управления
16. Протокол SNMP. Объекты SNMP, их параметры.
17. Протокол SNMP. Управляющая база MIB. Безопасность SNMP.
18. Групповая маршрутизация. Алгоритмы построения дерева доставки.
19. Групповая маршрутизация. Протоколы динамической групповой маршрутизации.
20. Управление доставкой. Коммутация 3-го уровня.
21. Качество обслуживание. Классификация приложений. Параметры качества обслуживания.
22. Архитектура службы QOS. Средства QoS. Протоколы сигнализации. Централизованные функции политики, управления и учета QoS.
23. Защита информации в компьютерных сетях. Виды нарушения защиты. Классификация сетевых атак. Механизмы защиты информации.

24. Криптографическая защита информации. Общие принципы симметричных систем шифрования. Алгоритмы замены и перестановки.

25. Криптографическая защита информации. Алгоритмы взбивания. Схема Фейстеля.

26. Криптографическая защита информации. Алгоритм DES. Режимы работы.

27. Криптографическая защита информации. Асимметричные системы шифрования. Понятие открытых и секретных ключей. Алгоритмы RSA и Эль-Гамаля.

28. Хэширование. Электронная цифровая подпись.

29. Механизмы защиты информации. Идентификация. Аутентификация.

30. Аутентификация на основе паролей. Аутентификация в ОС. Аудит.

31. Авторизация. Модели управления доступом. 32. Организация аутентификации на основе системы PAM.

33. Протоколы аутентификации и авторизации. PAP, CHAP, RADIUS, TACACS.

34. Архитектура системы Kerberos.

35. Криптографические файловые системы. Механизмы очистки «мусора».

36. Ограничение доступа к компьютерным сетям на основе межсетевых экранов (firewall). Типы экранов и их функции.

37. Виртуальные частные сети. (VPN). Архитектура IPSec.

38. Сертификация. Сертификаты. Удостоверяющие центры.

Критерии оценки (в баллах):

- «Зачтено» выставляется студенту, если он набрал по результатам изучения дисциплины 60 баллов;

- «Не зачтено» выставляется студенту, если он набрал менее 59 баллов.

4.3. 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

Основная литература:

1. Коноплева, И.А. Информационные технологии : учебное пособие / И.А. Коноплева, О.А. Хохлова, А.В. Денисов ; под ред. И.А. Коноплевой. - 2-е изд., перераб. и доп. - Москва : Проспект, 2014. - 328 с. - Библиогр. в кн. - ISBN 978-5-392-12385-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=251652

2. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - Санкт-Петербург : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040

3. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Режим доступа: https://e.lanbook.com/book/50578.

Дополнительная литература:

4. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. -

222 с. : ил. - Библиогр.: с. 214-215. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458204 .

5. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93245

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

1. Management. Учебно-методический комплекс – http://bgumanagement2009.narod.ru
2. Административно-управленческий портал – http://www.aup.ru
3. Архив Межуниверситетского Консорциума политических и социальных исследований (Interuniversity Consortium for Political and Social Research (ICPSR)) http://www.icpsr.umich.edu
4. Научная электронная библиотека https://elibrary.ru
5. Информационно-коммуникационные технологии в образовании http://www.ict.edu.ru/

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 занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус),	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 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

аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (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),		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 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.

компьютерный класс аудитория № 420 (гуманитарный корпус). **5. *помещения для самостоятельной работы:***аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).		

Приложение 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины Защита информации в компьютерных сетях на 9 семестр ОФО

Вид работы	Объем дисциплины	
	Очная форма обучения	Заочная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	6 ЗЕТ / 216 часов	-
Учебных часов на контактную работу с преподавателем:	72,2	-
лекций	36	-
практических / семинарских	36	-
лабораторных	-	-
контроль самостоятельной работы (КСР)	-	-
форма контактной работы (ФКР)	0,2	
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	143,8	-

Форма(ы) контроля:
Зачет 9 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / Сем	ЛР	СРС			
1	2	4	5	6	7	8	9	10
Модуль 1. **Основные понятия и положения защиты информации в системах связи**								
1	Альтернативные архитектуры КС. Архитектура сетей Novell. Альтернативные архитектуры КС. Архитектура DNA. Альтернативные архитектуры КС. Архитектура AppleTalk. Недостатки протокола IPv4. Семейство протоколов IPv6. Основные особенности. Протокол IPv6.	8	8	-	36	1-14	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Тест, лабораторная работа, практическая работа

	Адресация в сетях IPv6. Семейство протоколов IPv6. Сетевой уровень. Семейство протоколов IPv6. Маршрутизация, DNS, транспортные механизмы IPv6. Безопасность в IPv6. Способы совместного сосуществования сетей IPv4 и IPv6. Механизмы перехода на IPv6. Конфигурирование компьютерных сетей. Протоколы RARP, BOOTP, DHCP. Утилиты контроля и диагностики							
2	Управление учетом использования ресурсов. Управление неисправностями. Сетевые	8	8	-	36	1-14	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Тест, лабораторная работа, практическая работа

	анализаторы. Управление доставкой. Доступ к ресурсам с помощью серверов-посредников. Шлюзы уровня приложения (ALG). Управление доставкой. Протокол SOCKS. Управление доставкой. Технология трансляции адресов (NAT). Прозрачные серверыпосредники (transparent proxy). Туннелирование Управление в компьютерных сетях. Модель систем управления ISO. Архитектуры систем							

	управления							
Модуль 2. **Методы и средства защиты информации в системах связи**								
1	Протокол SNMP. Объекты SNMP, их параметры. Протокол SNMP. Управляющая база MIB. Безопасность SNMP. Групповая маршрутизация. Алгоритмы построения дерева доставки. Групповая маршрутизация. Протоколы динамической групповой маршрутизации. Управление доставкой. Коммутация 3-го уровня. Качество обслуживание. Классификация приложений. Параметры качества обслуживания	10	10	-	36	1-14	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	лабораторная работа, контрольная работа, практическая работа

2	Криптографическая защита информации. Общие принципы симметричных систем шифрования. Алгоритмы замены и перестановки. Криптографическая защита информации. Алгоритмы взбивания. Схема Фейстеля. Криптографическая защита информации. Алгоритм DES. Режимы работы. Криптографическая защита информации. Понятие открытых и секретных ключей. Алгоритмы RSA и Эль-Гамаля.	10	10	-	35,8	1-14	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	лабораторная работа, контрольная работа, практическая работа
		36	36		143,8			

Приложение 2

Рейтинг – план дисциплины

Защита информации в компьютерных сетях

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Курс 5, семестр 9

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Основные понятия и положения защиты информации в системах связи				
Текущий контроль			0	20
Лабораторная работа	10	1	0	10
Практическая работа	10	1	0	10
Рубежный контроль				
1. Тестовые задания	10	1	0	10
Всего			0	30
Модуль 2. Методы и средства защиты информации в системах связи				
Текущий контроль			0	30
Практическая работа	10	3	0	30
Рубежный контроль				
Лабораторная работа	10	3		30
Контрольная работа	10	1	0	10
Всего			0	40
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Зачет				
Итого			0	110