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

Утверждено:
на заседании кафедры
протокол № 9 от 24.04.2020
Зав. кафедрой / А.С. Исмагилова

Согласовано:
Председатель УМК института
/ Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Комплексная система защиты информации в правоохранительной сфере
Б1.В.1.ДВ.06.02 (вариативная)

Программа специалитета

Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация
Технологии защиты информации в правоохранительной сфере

Квалификация
Специалист по защите информации

Разработчик (составитель)
Доцент, канд.физ.-мат.наук,
доцент / Шагапов И.А.

Для приема: 2020 г.

Уфа 2020 г.

Составитель: И.А.Шагапов

Рабочая программа дисциплины утверждена на заседании кафедры управления информационной безопасностью
Протокол № 9 от 24.04.2020

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 (модулю):

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	Знать 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	ПК-1: способностью 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.	
	Знать характер воздействия вредных и опасных факторов на человека и природную среду, методы и способы защиты от них	ПК-12. Способность оказывать первую помощь, обеспечивать личную безопасность и безопасность граждан в процессе решения служебных задач.	
	Знать особенности защиты государственной тайны, состояние законодательной базы и стандарты в области защиты государственной тайны	ПК-30: Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации	
	Знать теоретические и методические основы организационной зашиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты	ПК-31: Способность принимать участие в создании системы защиты информации на объекте информатизации	

	государственной тайны, место и роль информационной безопасности в системе национальной безопасности Российской Федерации		
	Знать 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	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	
Умения	Уметь 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: способностью 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.	
	Уметь обеспечивать безопасность жизнедеятельности при осуществлении профессиональной деятельности и защите окружающей среды	ПК-12. Способность оказывать первую помощь, обеспечивать личную безопасность и безопасность граждан в процессе решения служебных задач.	
	Уметь обосновывать организационно-	ПК-30: Способность планировать проведение работ по комплексной	

	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	защите информации и сведений, составляющих государственную тайну, на объекте информатизации	
	Уметь осуществлять меры по организованной защите информации, 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	ПК-31: Способность принимать участие в создании системы защиты информации на объекте информатизации	
	Уметь 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	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	
Владения (навыки / опыт деятельности)	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач	ПК-1: способностью формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и	

	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 внедрения, адаптации и настройки средств защиты прикладных ИС	сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	
	Владеть основными методами защиты производственного персонала и населения при возникновении ЧС	ПК-12. Способность оказывать первую помощь, обеспечивать личную безопасность и безопасность граждан в процессе решения служебных задач.	
	Владеть навыками обоснования, выбора, реализации и контроля результатов управленческого решения, 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	ПК-30: Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации	
	Владеть навыками организации защиты	ПК-31: Способность принимать участие в создании системы защиты	

	информации, навыками организации и обеспечения режима секретности	информации на объекте информатизации	
	Владеть интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений, методологией и навыками решения научных и практических задач	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Комплексная система защиты информации в правоохранительной сфере» относится к дисциплинам по выбору вариативной части образовательной программы.

Дисциплина изучается на 3-ем курсе в 5 семестре.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «Математика», «Средства вычислительной техники», «Аппаратные средства вычислительной техники», «Средства и системы технического обеспечения обработки, хранения и передачи информации».

Целью учебной дисциплины «Комплексная система защиты информации в правоохранительной сфере» является формирование профессиональных компетенций у обучающихся в области комплексной системы защиты информации, методики и технологии ее организации, принципы и содержание управления системой, методов обеспечения ее надежности.

Полученные знания, навыки и умения используются при изучении дисциплин старших курсов, при прохождении производственной и преддипломной практик 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

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 политики, стратегии и технологии информационной безопасности и защиты	Не знает	Знает основы политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации

	информации, способы их организации и оптимизации		
	Знать общеметодологические принципы теории информационной безопасности	Не знает	Знает общеметодологические принципы теории информационной безопасности
	Знать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	Не знает	Знает возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации
	Знать состояние законодательной базы и стандарты в области информационной безопасности	Не знает	Знает состояние законодательной базы и стандарты в области информационной безопасности
Второй этап (уровень)	Уметь реализовывать на практике принципы политики безопасности	Не умеет	Имеет навыки реализации на практике принципов политики безопасности
	Уметь использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	Не умеет	Имеет навыки использования закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности
	Уметь	Не умеет	Имеет навыки обоснования

	обосновывать организационно-технические мероприятия по защите информации		организационно-технических мероприятий по защите информации
	Уметь использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	Не умеет	Имеет навыки использования возможностей и особенностей организационных, аппаратных и программных средств безопасности и защиты информации
Третий этап (уровень)	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	Не владеет	Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления
	Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	Не владеет	Владеет навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью
	Владеть навыками организации комплекса мероприятий по защите информации в процессах автоматизиро	Не владеет	Владеет навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации

	ванной обработки информации		
	Владеть навыками выявления и устранения угроз информационной безопасности	Не владеет	Владеет навыками выявления и устранения угроз информационной безопасности
	Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий	Не владеет	Владеет навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий
	Владеть навыками внедрения, адаптации и настройки средств защиты прикладных ИС	Не владеет	Владеет навыками внедрения, адаптации и настройки средств защиты прикладных ИС

ПК-12: Способность оказывать первую помощь, обеспечивать личную безопасность и безопасность граждан в процессе решения служебных 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 характер воздействия вредных и опасных факторов на человека и природную среду, методы	Не знает характер воздействия вредных и опасных факторов на человека и природную среду, методы и способы защиты от них	Знает характер воздействия вредных и опасных факторов на человека и природную среду, методы и способы защиты от них

	и способы защиты от них		
Второй этап (уровень)	Уметь обеспечивать безопасность жизнедеятельности при осуществлении профессиональной деятельности и защите окружающей среды	Не умеет обеспечивать безопасность жизнедеятельности при осуществлении профессиональной деятельности и защите окружающей среды	Умеет обеспечивать безопасность жизнедеятельности при осуществлении профессиональной деятельности и защите окружающей среды
Третий этап (уровень)	Владеть основными методами защиты производственного персонала и населения при возникновении ЧС	Не владеет основными методами защиты производственного персонала и населения при возникновении ЧС	Владеет основными методами защиты производственного персонала и населения при возникновении ЧС

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	Не знает	Знает особенности защиты государственной тайны
	Знать состояние законодательной базы и стандарты в области	Не знает	Знает состояние законодательной базы и стандарты в области защиты государственной тайны

	защиты государственной тайны		
Второй этап (уровень)	Уметь обосновывать организационно-технические мероприятия по защите государственной тайны	Не умеет	Имеет навыки обоснования организационно-технических мероприятий по защите государственной тайны
	Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу защиты государственной тайны	Не умеет	Умеет ориентироваться в нормативно-правовых актах, регламентирующих сферу защиты государственной тайны
	Уметь планировать внедрение и внедрять компоненты систем предприятия, обеспечивающих безопасность государственной тайны	Не умеет	Имеет навыки работы по планированию внедрения компонентов систем предприятия, обеспечивающих безопасность государственной тайны
Третий этап (уровень)	Владеть навыками обоснования, выбора, реализации и контроля результатов управленческого решения	Не владеет	Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения
	Владеть навыками выявления и устранения угроз информационной безопасности	Не владеет	Владеет навыками выявления и устранения угроз информационной безопасности

	Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий	Не владеет	Владеет навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий
	Владеть навыками внедрения, адаптации и настройки средств защиты прикладных ИС	Не владеет	Владеет навыками внедрения, адаптации и настройки средств защиты прикладных ИС

ПК-31: Способность принимать участие в создании системы защиты информации 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 теоретические и методические основы организационной зашиты информации	Не знает	Демонстрирует целостные знания о теоретических и методических основах организационной зашиты информации
	Знать правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи	Не знает	Демонстрирует целостные знания о правовых основах организации защиты государственной тайны и конфиденциальной информации, задачах органов защиты государственной тайны

	органов защиты государственной тайны		
	Знать место и роль информационной безопасности в системе национальной безопасности Российской Федерации	Не знает	Демонстрирует целостные знания о месте и роли информационной безопасности в системе национальной безопасности Российской Федерации
Второй этап (уровень)	Уметь осуществлять меры по организованной защите информации	Не умеет	Умеет осуществлять меры по организованной защите информации
	Уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	Не умеет	Умеет формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе
	Уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Не умеет	Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
Третий	Владеть	Не владеет	Способен использовать

этап (уровень)	навыками организации защиты информации		навыки организации защиты информации
	Владеть навыками организации и обеспечения режима секретности	Не владеет	Способен использовать навыки организации и обеспечения режима секретности

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 нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом	Не знает	Знает нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом
	Знать стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов	Не знает	Знает стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов
	Знать	Не знает	Знает методики анализа

	методики анализа рисков информационных систем		рисков информационных систем
Второй этап (уровень)	Уметь интерпретировать и обобщать данные, формулировать выводы и рекомендации	Не умеет	Имеет навыки интерпретации и обобщения данных, формулирования выводов и рекомендаций
	Уметь применять на практике методы обработки данных	Не умеет	Умеет применять на практике методы обработки данных
	Уметь разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	Не умеет	Имеет навыки работы по разработке и реализации решений, направленных на поддержку социально-значимых проектов и развитие компьютерного творчества
Третий этап (уровень)	Владеть навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	Не владеет	Владеет навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений
	Владеть методологией и навыками решения научных и практических задач	Не владеет	Владеет методами и навыками решения научных и практических задач

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 50 баллов; рубежный контроль – максимум 50 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 этап Знания	Знать 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	ПК-1: способностью 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.	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Знать характер воздействия вредных и опасных факторов на человека и природную среду, методы и способы защиты от них	ПК-12. Способность оказывать первую помощь, обеспечивать личную безопасность и безопасность граждан в процессе решения служебных задач.	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Знать особенности защиты государственной тайны, состояние	ПК-30: Способность планировать проведение работ по комплексной защите информации и сведений,	Практическое задание, Письменная

	законодательной базы и стандарты в области защиты государственной тайны	составляющих государственную тайну, на объекте информатизации	контрольная работа, Лабораторная работа
	Знать теоретические и методические основы организационной зашиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны, место и роль информационной безопасности в системе национальной безопасности Российской Федерации	ПК-31: Способность принимать участие в создании системы защиты информации на объекте информатизации	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Знать 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	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Практическое задание, Письменная контрольная работа, Лабораторная работа
2 этап Умения	Уметь 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	ПК-1: способностью 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.	Практическое задание, Письменная контрольная работа, Лабораторная работа

	организационных, аппаратных и программных средств безопасности и защиты информации		
	Уметь обеспечивать безопасность жизнедеятельности при осуществлении профессиональной деятельности и защите окружающей среды	ПК-12. Способность оказывать первую помощь, обеспечивать личную безопасность и безопасность граждан в процессе решения служебных задач.	Практическое задание, Письменная контрольная работа, Лабораторная работа
	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	ПК-30: Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Уметь осуществлять меры по организованной защите информации, 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	ПК-31: Способность принимать участие в создании системы защиты информации на объекте информатизации	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Уметь интерпретировать и обобщать данные, формулировать выводы и рекомендации,	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной	Практическое задание, Письменная контрольная

	применять на практике методы обработки данных, разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	безопасности	работа, Лабораторная работа
3 этап Владения (навыки / опыт деятельности)	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 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	ПК-1: способностью 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.	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Владеть основными методами защиты производственного персонала и населения при возникновении ЧС	ПК-12. Способность оказывать первую помощь, обеспечивать личную безопасность и безопасность граждан в процессе решения служебных задач.	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Владеть навыками обоснования, выбора, реализации и контроля результатов управленческого	ПК-30: Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации	Практическое задание, Письменная контрольная работа,

	решения, 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		Лабораторная работа
	Владеть навыками организации защиты информации, навыками организации и обеспечения режима секретности	ПК-31: Способность принимать участие в создании системы защиты информации на объекте информатизации	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Владеть интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений, методологией и навыками решения научных и практических задач	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Практическое задание, Письменная контрольная работа, Лабораторная работа

Типовые вопросы к зачету

1. Сущность и задачи комплексной защиты информации
2. Понятийный аппарат в области обеспечения безопасности информации
3. Цели, задачи и принципы построения КСЗИ
4. Принципы организации и этапы разработки КСЗИ
5. Методологические основы организации КСЗИ
6. Требования, предъявляемые к КСЗИ
7. Этапы разработки КСЗИ
8. Факторы, влияющие на организацию КСЗИ
9. Факторы, определяющие необходимость защиты периметра и здания предприятия
10. Особенности помещений как объектов защиты для работы по защите информации
11. Транспортные средства и особенности транспортировки
12. Состав средств обеспечения, подлежащих защите
13. Дестабилизирующие воздействия на информацию и их нейтрализация
14. Факторы, создающие угрозу информационной безопасности
15. Угрозы безопасности информации
16. Модели нарушителей безопасности АС
17. Подходы к оценке ущерба от нарушений ИБ

18. Обеспечение безопасности информации в непредвиденных ситуациях
19. Реагирование на инциденты ИБ
20. Резервирование информации и отказоустойчивость
21. Определение потенциальных каналов и методов несанкционированного доступа к информации
22. Задачи КСЗИ по выявлению угроз и КУИ
23. Особенности защиты речевой информации
24. Определение возможностей несанкционированного доступа к защищаемой информации
25. Методы и способы защиты информации
26. Классификация СЗИ НСД
27. Механизмы обеспечения безопасности информации
28. Разграничение доступа. Регистрация и аудит
29. Методика выявления нарушителей, тактики их действий и состава интересующей их информации
30. Определение компонентов КСЗИ
31. Методика синтеза СЗИ
32. Проектирование системы защиты информации для существующей АС
33. Определение условий функционирования КСЗИ
34. Содержание концепции построения КСЗИ
35. Объекты защиты. Цели и задачи обеспечения безопасности информации
36. Основные положения технической политики в области обеспечения безопасности информации АС организации
37. Основные принципы построения КСЗИ
38. Разработка модели КСЗИ
39. Общая характеристика задач моделирования КСЗИ
40. Формальные модели безопасности и их анализ
41. Формализация модели безопасности
42. Технологическое и организационное построение КСЗИ
43. Характеристика основных стадий создания КСЗИ
44. Кадровое обеспечение функционирования комплексной системы защиты информации
45. . Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа
46. Подбор и обучение персонала
47. Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации
48. Перечень вопросов ЗИ, требующих документационного закрепления
49. Назначение, структура и содержание управления КСЗИ
50. Принципы и методы планирования функционирования КСЗИ. Сущность и содержание контроля функционирования
51. Проведение контрольных мероприятий в КСЗИ
52. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций. Технология принятия решений в условиях ЧС.
53. Факторы, влияющие на принятие решений в условиях ЧС. Подготовка мероприятий на случай возникновения ЧС
54. Общая характеристика подходов к оценке эффективности КСЗИ. Методы и модели оценки эффективности КСЗИ
55. Показатель уровня защищенности, основанный на экспертных оценках. Методы проведения экспертного опроса

56. Экономический подход к оценке эффективности КСЗИ

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.

Комплект контрольных работ

Для контроля освоения и/или расширения знаний, умений, владений предусмотрены несколько контрольных работ.

Модуль 1
Разработка модели КСЗИ в ПС

Письменная контрольная работа №1
Угрозы и уязвимости информационной безопасности
Вопросы

1. Зайти на сайт ФСТЭК, изучить содержание сайта

2. Выбрать на свое усмотрение 3-4 угрозы и 3-4 уязвимости из предложенного на сайте банка

3. Изучить их и подготовить краткий отчет.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	6
Выполнены пункты 1-3	10
Максимальный балл	10

Модуль 2.
Характеристика подходов к оценке эффективности КСЗИ в ПС

Письменная контрольная работа№2
Разработка КСЗИ

Вопросы

1. Принципы организации и этапы разработки КСЗИ
2. Система управления информационной безопасностью предприятия.
3. Требования, предъявляемые к КСЗИ. Этапы разработки КСЗИ

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	6
Выполнены пункты 1-3	10
Максимальный балл	10

Комплект практических заданий

Для самостоятельного освоения и/или расширения знаний, умений, владений предусмотрены несколько практических заданий.

Модуль 1

Разработка модели КСЗИ в ПС

Типовое практическое задание 1

Задание 1. Модель угроз информационной безопасности

1. Выбрать объект защиты (документ, АРМ, ПК, помещение, АС и т.д.).
2. Собрать необходимую информацию.
3. Построить модель угроз информационной безопасности.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 50%	6
Выполнены пункты 100%	10
Максимальный балл	10

Модуль 2.

Характеристика подходов к оценке эффективности КСЗИ в ПС

Типовое практическое задание 2

Задание 2. Модель нарушителя информационной безопасности

1. Выбрать объект защиты (документ, АРМ, ПК, помещение, АС и т.д.).
2. Собрать необходимую информацию.
3. Построить модель нарушителя безопасности.

Методические указания

а. Использовать известные уровни возможностей нарушителя, различные классификации нарушителя.

б. Помнить, для чего строится модель нарушителя.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 50%	6
Выполнены пункты 100%	10
Максимальный балл	10

Комплект лабораторных работ

Для закрепления на практике знаний, умений, владений предусмотрены несколько лабораторных работ.

Модуль 1
Разработка модели КСЗИ в ПС

Типовая лабораторная работа 1
Правовой защита информации

1. Для предприятия, выбранного согласно вашему варианту, составить список нормативных правовых актов и стандартов, которыми необходимо руководствоваться при построении комплексной системы защиты информации предприятия. К каждому документу представить комментарий, указывающий обязательный или рекомендательный характер документа, основное содержание документа, область применения документа для рассматриваемого вами предприятия.
   Варианты:
   1. железнодорожная станция;
   6. школа;
   7. библиотека;
   8. юридическая фирма;
   9. фирма по разработке программного обеспечения
2. Составить отчет по работе

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 50%	6
Выполнены пункты 100%	10
Максимальный балл	10

Модуль 1
Разработка модели КСЗИ в ПС

Типовая лабораторная работа 2
Модель угроз информационной безопасности

1. Выбрать объект защиты (документ, АРМ, ПК, помещение, АС и т.д.).
2. Собрать необходимую информацию.
3. Построить модель угроз информационной безопасности.
4. Составить отчет по работе

Методические указания

а. Использовать известные уровни возможностей реализации угроз, различные классификации угроз.

б. Помнить, для чего строится модель угроз.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	6
Выполнены пункты 1-4	10
Максимальный балл	10

Модуль 2.
Характеристика подходов к оценке эффективности КСЗИ в ПС

Типовая лабораторная работа 3
Модель нарушителя информационной безопасности

1. Выбрать объект защиты (документ, АРМ, ПК, помещение, АС и т.д.).
2. Собрать необходимую информацию.
3. Построить модель нарушителя безопасности.
4. Составить отчет по работе

Методические указания

а. Использовать известные уровни возможностей нарушителя, различные классификации нарушителя.

б. Помнить, для чего строится модель нарушителя.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	6
Выполнены пункты 1-4	10
Максимальный балл	10

Модуль 2.
Характеристика подходов к оценке эффективности КСЗИ в ПС.

Типовая лабораторная работа 4

Разработка технического задания (ТЗ) в области информационной безопасности

1. Выбрать вариант для написания ТЗ объект (услуга, работа, разработка, модификация и т.д. в области ИБ)
2. Собрать необходимую информацию.
3. Разработать техническое задание.
4. Составить отчет по работе

Методические указания

а. Изучить ГОСТ по написанию ТЗ и образцы готовых вариантов.

б. Помнить, для чего и для кого разрабатывается ТЗ.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	6
Выполнены пункты 1-4	10
Максимальный балл	10

4.3. Рейтинг-план дисциплины

Рейтинг-план дисциплины представлен в приложении 2.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. 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
2. Организация безопасной работы информационных систем : учебное пособие / Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др. ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=277794
3. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва : Издательский дом Высшей школы экономики, 2015. - 574 с. : ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285

Дополнительная литература

4. Больбат, Е.П. ПРООЕКТИРОВАНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ (КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ). [Электронный ресурс] — Электрон. дан. // Вестник научного общества студентов, аспирантов и молодых ученых. — 2015. — № 3. — С. 21-25. — Режим доступа: http://e.lanbook.com/journal/issue/294140
5. Масалков, А.С. Особенности киберпреступлений: инструменты нападения и защиты информации [Электронный ресурс] / А.С. Масалков. — Электрон. дан. — Москва : ДМК Пресс, 2018. — 226 с. — Режим доступа: https://e.lanbook.com/book/105842. — Загл. с экрана.

6. Степанов-Егиянц, В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации [Электронный ресурс] : монография / В.Г. Степанов-Егиянц. — Электрон. дан. — Москва : СТАТУТ, 2016. — 190 с. — Режим доступа: https://e.lanbook.com/book/92503. — Загл. с экрана.
7. Бойченко, О.В. ПРОБЛЕМАТИКА КОМПЛЕКСНОЙ ОЦЕНКИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ [Электронный ресурс] / О.В. Бойченко, Б.В. Белименко. // Ученые записки Крымского федерального университета им. В.И. Вернадского. Экономика и управление. — Электрон. дан. — 2015. — № 1. — С. 27-31. — Режим доступа: https://e.lanbook.com/journal/issue/299849. — Загл. с экрана.

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

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

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1. *учебная аудитория для проведения занятий лекционного типа:* аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус),	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

аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2.** ***учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **3.** ***учебная аудитория для 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).		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 APAPT MA1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт APAPT MA1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/ Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.

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:***аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).		**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.

Приложение 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины Комплексная система защиты информации в правоохранительной сфере
на 5 семестр - ОФО

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	54,2
лекций	18
практических / семинарских	18
лабораторных	18
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	0,2
Учебных часов на самостоятельную работу	53,8
Учебных часов на подготовку к / зачету	

Форма(ы) контроля:
Зачет 5 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)					Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
			ЛК	ПР / Сем	ЛР	СРС			
1	2		4	5	6	7	8	9	10
1	**Сущность и задачи комплексной защиты информации** Принципы организации и этапы разработки КСЗИ Факторы, влияющие на организацию КСЗИ Определение и нормативное закрепление состава защищаемой информации Определение объектов защиты		2	2		6	1-7	Изучить вопросы определения несанкционированного доступа к защищаемой информации	Практическое задание, Письменная контрольная работа
2	Дестабилизирующие воздействия на информацию и их нейтрализация Определение потенциальных каналов и методов несанкционированного		2	2	4	6	1-6	Изучить возможности несанкционированного доступа к защищаемой информации	Практическое задание, Письменная контрольная работа, Лабораторная работа

	доступа к информации Определение компонентов КСЗИ Определение условий функционирования КСЗИ								
3	**Разработка модели КСЗИ** Технологическое и организационное построение КСЗИ Кадровое обеспечение функционирования комплексной системы защиты информации		2	2		6	179	Изучить актуальные вопросы построения КСЗИ	Практическое задание, Письменная контрольная работа
4	Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации		2	2	4	6	1-7	Изучить вопросы оправданности построения КСЗИ	Практическое задание, Письменная контрольная работа, Лабораторная работа
5	**Назначение, структура и содержание управления КСЗИ** Принципы и методы планирования функционирования КСЗИ		2	2	4	6	1-7	Изучить правовые аспекты защиты информации в условиях чрезвычайных ситуаций	Практическое задание, Письменная контрольная работа, Лабораторная работа
6	Сущность и содержание контроля функционирования Управление		2	2		6	1-6	Оценить эффективность правовых аспектов защиты	Практическое задание, Письменная контрольная

	комплексной системой защиты информации в условиях чрезвычайных ситуаций							информации в условиях чрезвычайных ситуаций	работа
7	**Общая характеристика подходов к оценке эффективности КСЗИ** Методы и модели оценки эффективности КСЗИ		2	2	2	6	1-7	Изучить отечественный опыт подходов к оценке эффективности КСЗИ	Практическое задание, Письменная контрольная работа, Лабораторная работа
8	Показатель уровня защищенности, основанный на экспертных оценках Методы проведения экспертного опроса		2	2	2	6	1-7	Изучить зарубежный опыт подходов к оценке эффективности КСЗИ	Практическое задание, Письменная контрольная работа, Лабораторная работа
9	Экономический подход к оценке эффективности КСЗИ		2	2	2	5,8	1-7	Сравнить отечественный и зарубежный опыт подходов к оценке эффективности КСЗИ	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Всего		18	18	18	53,8			

Приложение 2

Рейтинг – план дисциплины

Комплексная система защиты информации в правоохранительной сфере

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Курс 3, семестр 5

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Разработка модели КСЗИ в ПС				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №1	10	1	0	10
3. Лабораторная работа №1	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №1	10	1	0	10
2 Лабораторная работа №2	10	1	0	10
Всего				50
Модуль 2. Характеристика подходов к оценке эффективности КСЗИ в ПС				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №2	10	1	0	10
3.Лабораторная работа №3	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №2	10	1	0	10
2 Лабораторная работа №4	10	1	0	10
Всего				50
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				0