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

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

Согласовано:
Председатель УМК института
/Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Комплексная система защиты информации на предприятии
Б1.Б.29 базовая

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации

Квалификация
бакалавр

Разработчик (составитель)
к.ф.-м.н., доцент
/И.А. Шагапов

Для приема: 2015 г.

Уфа 2018 г.

Составитель: доцент И.А. Шагапов

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью
Протокол № 10 от «07» июня 2018 г.

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

Заведующий кафедрой ___________________/ _____________Ф.И.О/

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

Заведующий кафедрой ___________________/ _____________Ф.И.О/

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

Заведующий кафедрой ___________________/ _____________Ф.И.О/

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

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Список документов и материалов

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

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

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	Знать базовые экономические понятия (спрос, предложение, цена, стоимость, товар, деньги, доходы, расходы, прибыль, риск, собственность, управление, рынок, фирма, государство)	ОК-2. Способность использовать основы экономических знаний в различных сферах деятельности	
	Знать средства контроля контента, средства анализа защищенности и средства обнаружения атак, средства защиты от несанкционированного доступа	ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности, возможности и особенности организационных средств безопасности и защиты информации, состояние законодательной базы и стандарты в области информационной безопасности	ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
	Знать правовые основы организации защиты государственной тайны и конфиденциальной информации	ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	
	Знать понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	
	Знать общеметодологические принципы теории информационной безопасности	ПСК-2. Способность разрабатывать предложения по совершенствованию системы	

		управления информационной безопасностью	
	Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации, нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	ПК-15. Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	
Умения	Уметь решать типичные задачи, связанные с личным финансовым планированием (рассчитать процентные ставки, оценить целесообразность взятия кредита с точки зрения текущих и будущих доходов и расходов, оценить эффективность страхования)	ОК-2. Способность использовать основы экономических знаний в различных сферах деятельности	
	Уметь использовать базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность	ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
	Уметь реализовывать на практике принципы политики безопасности, использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
	Уметь разрабатывать организационно-распорядительные документы по вопросам защиты информации	ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	
	Уметь использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	
	Уметь обосновывать организационно-технические мероприятия по защите информации.	ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной	

		безопасностью	
	Уметь анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности	ПК-15. Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	
Владения (навыки / опыт деятель-ности)	Владеть методами личного финансового планирования (бюджетирование, оценка будущих доходов и расходов, сравнение условий различных финансовых продуктов, управление рисками, применение инструментов защиты прав потребителя финансовых услуг)	ОК-2. Способность использовать основы экономических знаний в различных сферах деятельности	
	Владеть методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам	ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
	Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности	ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	
	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	ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	
	Владеть навыками обоснования, выбора, реализации и контроля результатов управленческого решения	ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью	

	Владеть навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности, навыками обеспечения и соблюдения режима секретности	ПК-15. Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Комплексная система защиты информации на предприятии» относится к обязательным дисциплинам базовой части.

Дисциплина изучается на 3,4 курсах в 6,7 семестрах.

Целью освоения дисциплины «Комплексная система защиты информации на предприятии» является формирование профессиональных компетенций у обучающихся в области комплексной системы защиты информации, методики и технологии ее организации, принципов управления, методов обеспечения ее надежности.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «Документоведение», «Программно-аппаратные средства защиты информации», «Организационное и правовое обеспечение информационной безопасности», «Техническая защита информации», «Экономика защиты информации», «Информационные технологии».

Полученные знания, навыки и умения используются при изучении дисциплин старших курсов, 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

ОК-2. Способность использовать основы экономических знаний в различных сферах деятельности

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов экзамена и защиты курсового проекта			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать базовые экономические понятия (спрос, предложение, цена, стоимость, товар, деньги, доходы, расходы, прибыль, риск, собственность,	Фрагментарно знает базовые экономические понятия (спрос, предложение, цена, стоимость, товар, деньги, доходы, расходы,	В целом знает базовые экономические понятия (спрос, предложение, цена, стоимость, товар, деньги, доходы, расходы,	Знает базовые экономические понятия (спрос, предложение, цена, стоимость, товар, деньги, доходы, расходы, прибыль,	Уверенно знает базовые экономические понятия (спрос, предложение, цена, стоимость, товар, деньги, доходы, расходы,

	управление, рынок, фирма, государство)	прибыль, риск, собственность, управление, рынок, фирма, государство)	прибыль, риск, собственность, управление, рынок, фирма, государство)	риск, собственность, управление, рынок, фирма, государство)	прибыль, риск, собственность, управление, рынок, фирма, государство)
Второй этап (уровень)	Уметь решать типичные задачи, связанные с личным финансовым планированием (рассчитать процентные ставки, оценить целесообразность взятия кредита с точки зрения текущих и будущих доходов и расходов, оценить эффективность страхования)	Не показывает сформированные умения решать типичные задачи, связанные с личным финансовым планированием (рассчитать процентные ставки, оценить целесообразность взятия кредита с точки зрения текущих и будущих доходов и расходов, оценить эффективность страхования)	Умеет использовать некоторые приемы решать типичные задачи, связанные с личным финансовым планированием (рассчитать процентные ставки, оценить целесообразность взятия кредита с точки зрения текущих и будущих доходов и расходов, оценить эффективность страхования)	Уверенно использует большинство приемов решать типичные задачи, связанные с личным финансовым планированием (рассчитать процентные ставки, оценить целесообразность взятия кредита с точки зрения текущих и будущих доходов и расходов, оценить эффективность страхования)	Уверенно умеет решать типичные задачи, связанные с личным финансовым планированием (рассчитать процентные ставки, оценить целесообразность взятия кредита с точки зрения текущих и будущих доходов и расходов, оценить эффективность страхования)
Третий этап (уровень)	Владеть методами личного финансового планирования (бюджетирование, оценка будущих доходов и расходов, сравнение условий различных финансовых продуктов, управление рисками, применение инструментов защиты прав потребителя финансовых услуг)	Не владеет основными методами личного финансового планирования (бюджетирование, оценка будущих доходов и расходов, сравнение условий различных финансовых продуктов, управление рисками, применение инструментов защиты прав потребителя финансовых услуг)	Владеет основными методами личного финансового планирования (бюджетирование, оценка будущих доходов и расходов, сравнение условий различных финансовых продуктов, управление рисками, применение инструментов защиты прав потребителя финансовых услуг), но допускает	Владеет основными методами личного финансового планирования (бюджетирование, оценка будущих доходов и расходов, сравнение условий различных финансовых продуктов, управление рисками, применение инструментов защиты прав потребителя финансовых услуг)	Уверенно владеет методами личного финансового планирования (бюджетирование, оценка будущих доходов и расходов, сравнение условий различных финансовых продуктов, управление рисками, применение инструментов защиты прав потребителя финансовых услуг)

			ошибки		

ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов экзамена и защиты курсового проекта			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать средства контроля контента, средства анализа защищенности и средства обнаружения атак, средства защиты от несанкционированного доступа	Фрагментарно знает основные средства контроля контента, средства анализа защищенности и средства обнаружения атак, средства защиты от несанкционированного доступа	В целом знает основные средства контроля контента, средства анализа защищенности и средства обнаружения атак, средства защиты от несанкционированного доступа	Знает основные средства контроля контента, средства анализа защищенности и средства обнаружения атак, средства защиты от несанкционированного доступа	Уверенно знает основные средства контроля контента, средства анализа защищенности и средства обнаружения атак, средства защиты от несанкционированного доступа
Второй этап (уровень)	Уметь использовать базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность	Не показывает сформированные умения использовать базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность	Умеет использовать некоторые приемы использовать базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность	Уверенно использует большинство приемов использовать базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность	Уверенно использует базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность

Третий этап (уровень)	Владеть методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам	Не владеет основными навыками определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам	Владеет основными навыками определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам, но допускает ошибки	Владеет основными навыками определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам	Уверенно владеет методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам

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

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов экзамена и защиты курсового проекта			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности, возможности и особенности организационных средств безопасности и защиты информации, состояние законодательно	Фрагментарно знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности, возможности и особенности организационных средств безопасности и защиты информации, состояние	В целом знает основные политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности, возможности и особенности организационных средств безопасности и защиты информации, состояние	Знает основные политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности, возможности и особенности организационных средств безопасности и защиты информации, состояние	Уверенно знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности, возможности и особенности организационных средств безопасности и защиты информации, состояние

	й базы и стандарты в области информационн ой безопасности	законодательн ой базы и стандарты в области информацион ной безопасности	законодательн ой базы и стандарты в области информацион ной безопасности	законодательн ой базы и стандарты в области информацион ной безопасности	законодательн ой базы и стандарты в области информацион ной безопасности
Второй этап (уровень)	Уметь реализовывать на практике принципы политики безопасности, использовать закономерност и преобразовани я данных в каналах при выполнении комплекса мер по информационн ой безопасности	Не показывает сформированн ые умения реализовывать на практике принципы политики безопасности, использовать закономерност и преобразовани я данных в каналах при выполнении комплекса мер по информацион ной безопасности.	Умеет использовать некоторые методы реализовывать на практике принципы политики безопасности, использовать закономерност и преобразовани я данных в каналах при выполнении комплекса мер по информацион ной безопасности	Уверенно использует большинство методов реализовывать на практике принципы политики безопасности, использовать закономерност и преобразовани я данных в каналах при выполнении комплекса мер по информацион ной безопасности	Уверенно умеет реализовывать на практике принципы политики безопасности, использовать закономерност и преобразовани я данных в каналах при выполнении комплекса мер по информацион ной безопасности
Третий этап (уровень)	Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационн ой безопасностью, навыками выявления и устранения угроз информационн ой безопасности	Не владеет навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информацион ной безопасность ю, навыками выявления и устранения угроз информацион ной безопасности	Владеет основными навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информацион ной безопасность ю, навыками выявления и устранения угроз информацион ной безопасности	Владеет основными навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информацион ной безопасность ю, навыками выявления и устранения угроз информацион ной безопасности	Уверенно владеет навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информацион ной безопасностью , навыками выявления и устранения угроз информацион ной безопасности

ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

Этап (уровень) освоения компетенци и	Планируемые результаты обучения (показатели достижения	Критерии оценивания результатов экзамена и защиты курсового проекта			
		2 («Не удовлетворите льно»)	3 («Удовлетвор ительно»)	4 («Хорошо»)	5 («Отлично»)

	заданного уровня освоения компетенций)				
Первый этап (уровень)	Знать правовые основы организации защиты государственной тайны и конфиденциальной информации	Фрагментарно знает правовые основы организации защиты государственной тайны и конфиденциальной информации	В целом знает правовые основы организации защиты государственной тайны и конфиденциальной информации	Знает правовые основы организации защиты государственной тайны и конфиденциальной информации	Уверенно знает правовые основы организации защиты государственной тайны и конфиденциальной информации
Второй этап (уровень)	Уметь разрабатывать организационно-распорядительные документы по вопросам защиты информации	Не показывает сформированные умения разрабатывать организационно-распорядительные документы по вопросам защиты информации	Умеет использовать некоторые методы разработки организационно-распорядительные документы по вопросам защиты информации	Уверенно использует большинство методов разработки организационно-распорядительные документы по вопросам защиты информации	Уверенно умеет разрабатывать организационно-распорядительные документы по вопросам защиты информации
Третий этап (уровень)	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Не владеет основными навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Владеет основными навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации, но допускает значительные ошибки.	Владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Уверенно владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации

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

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

Первый этап (уровень)	Знать: правила подключения охранных и пожарных датчиков к приемно-контрольным панелям и принципы программирования приемно-контрольных панелей; достоинства и недостатки различного оборудования используемого в системах наблюдения; принципы построения систем контроля и ограничения доступа и регистрацию в них пользователей, основные правила эксплуатации досмотрового и антитеррористического оборудования, политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	Фрагментарно знает основные правила подключения охранных и пожарных датчиков к приемно-контрольным панелям и принципы программирования приемно-контрольных панелей; достоинства и недостатки различного оборудования используемого в системах наблюдения; принципы построения систем контроля и ограничения доступа и регистрацию в них пользователей, основные правила эксплуатации досмотрового и антитеррористического оборудования.	В целом знает основные правила подключения охранных и пожарных датчиков к приемно-контрольным панелям и принципы программирования приемно-контрольных панелей; достоинства и недостатки различного оборудования используемого в системах наблюдения; принципы построения систем контроля и ограничения доступа и регистрацию в них пользователей, основные правила эксплуатации досмотрового и антитеррористического оборудования.	Знает основные правила подключения охранных и пожарных датчиков к приемно-контрольным панелям и принципы программирования приемно-контрольных панелей; достоинства и недостатки различного оборудования используемого в системах наблюдения; принципы построения систем контроля и ограничения доступа и регистрацию в них пользователей, основные правила эксплуатации досмотрового и антитеррористического оборудования.	Уверенно знает основные правила подключения охранных и пожарных датчиков к приемно-контрольным панелям и принципы программирования приемно-контрольных панелей; достоинства и недостатки различного оборудования используемого в системах наблюдения; принципы построения систем контроля и ограничения доступа и регистрацию в них пользователей, основные правила эксплуатации досмотрового и антитеррористического оборудования.
Второй этап (уровень)	Уметь: подключать охранные и пожарные датчики к приемно-контрольным панелям с разным числом	Не показывает сформированные умения подключения, настройки и конфигурирования технических средств	Умеет использовать некоторые методы подключения, настройки и конфигурирования технических	Уверенно использует большинство методов подключения, настройки и конфигурирования технических	Уверенно использует методы подключения, настройки и конфигурирования технических средств

	датчиков в шлейфе; настраивать системы видеонаблюдения с точки зрения угла обзора камер, реакции на события в поле зрения камер, расписания работы; создавать конфигурацию системы контроля и ограничения доступа в центральном компьютере системы; создавать списки пользователей системы с определенными ограничениями по времени доступа и прохода в разные помещения, реализовывать на практике принципы политики безопасности	охраны	средств охраны	средств охраны.	охраны.
Третий этап (уровень)	Владеть: монтажа и настройки технических средств охраны объектов; составлять сметную документацию на оснащение помещений техническими средствами защиты информации; профессиональной терминологией	Не владеет основными методами монтажа и настройки технических средств охраны объектов; составлять сметную документацию на оснащение помещений техническими средствами защиты информации;	Владеет основными методами монтажа и настройки технических средств охраны объектов; составлять сметную документацию на оснащение помещений техническими средствами защиты информации;	Владеет основными методами монтажа и настройки технических средств охраны объектов; составлять сметную документацию на оснащение помещений техническими средствами защиты информации;	Уверенно владеет основными методами монтажа и настройки технических средств охраны объектов; составлять сметную документацию на оснащение помещений техническими средствами защиты

	, навыками анализа, обработки и интерпретации результатов решения прикладных задач управления;	профессиональной терминологией	профессиональной терминологией, но допускает значительные ошибки.	профессиональной терминологией	информации; профессиональной терминологией

ПК-15. Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов экзамена и защиты курсового проекта			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации, нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	Фрагментарно знает основные нормативные и правовые акты в области информационной безопасности и защиты информации, нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	В целом знает основные нормативные и правовые акты в области информационной безопасности и защиты информации, нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	Знает основные нормативные и правовые акты в области информационной безопасности и защиты информации, нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	Уверенно знает основные нормативные и правовые акты в области информационной безопасности и защиты информации, нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области
Второй этап (уровень)	Уметь анализировать и составлять основные правовые акты и осуществлять правовую	Не показывает сформированные умения анализировать и составлять основные правовые акты	Умеет использовать некоторые методы анализировать и составлять основные	Уверенно использует большинство методов анализировать и составлять основные	Уверенно умеет анализировать и составлять основные правовые акты и

	оценку информации, используемых в профессиональной деятельности, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности	и осуществлять правовую оценку информации, используемых в профессиональной деятельности, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности	правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности	правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности	осуществлять правовую оценку информации, используемых в профессиональной деятельности, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности
Третий этап (уровень)	Владеть навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности, навыками обеспечения и соблюдения режима секретности	Не владеет основными навыками работы с нормативным и правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности, навыками обеспечения и соблюдения режима секретности	Владеет основными навыками работы с нормативным и правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности, навыками обеспечения и соблюдения режима секретности, но допускает значительные ошибки.	Владеет навыками работы с нормативным и правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности, навыками обеспечения и соблюдения режима секретности	Уверенно владеет навыками работы с нормативным и правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности, навыками обеспечения и соблюдения режима секретности

ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения	Критерии оценивания результатов экзамена и защиты курсового проекта			
		2 («Не удовлетворите	3 («Удовлетвор	4 («Хорошо»)	5 («Отлично»)

	заданного уровня освоения компетенций)	льно»)	ительно»)		
Первый этап (уровень)	Знать состояние законодательной базы и стандарты в области информационной безопасности, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, тенденции и перспективы развития систем защиты информации в ведущих зарубежных странах	Фрагментарно знает состояние законодательной базы и стандарты в области информационной безопасности, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, тенденции и перспективы развития систем защиты информации в ведущих зарубежных странах	В целом знает состояние законодательной базы и стандарты в области информационной безопасности, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, тенденции и перспективы развития систем защиты информации в ведущих зарубежных странах	Знает основы состояния законодательной базы и стандарты в области информационной безопасности, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, тенденции и перспективы развития систем защиты информации в ведущих зарубежных странах	Уверенно знает состояние законодательной базы и стандарты в области информационной безопасности, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации, тенденции и перспективы развития систем защиты информации в ведущих зарубежных странах
Второй этап (уровень)	Уметь: обосновывать организационно-технические мероприятия по защите информации.	Не показывает сформированные умения обосновывать организационно-технические мероприятия по защите информации	Умеет использовать некоторые методы обосновывать организационно-технические мероприятия по защите информации	Уверенно использует большинство методов обосновывать организационно-технические мероприятия по защите информации	Уверенно умеет обосновывать организационно-технические мероприятия по защите информации
Третий этап (уровень)	Владеть: навыками обоснования, выбора, реализации и контроля результатов управленческого решения, навыками выявления и	Не владеет основными навыками обоснования, выбора, реализации и контроля результатов управленческого решения, навыками	Владеет основными навыками обоснования, выбора, реализации и контроля результатов управленческого решения, навыками	Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения, навыками выявления и	Уверенно владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения, навыками

	устранения угроз информационной безопасности; эксплуатации современного электронного оборудования и информационно-коммуникационных технологий	выявления и устранения угроз информационной безопасности; эксплуатации современного электронного оборудования и информационно-коммуникационных технологий	выявления и устранения угроз информационной безопасности; эксплуатации современного электронного оборудования и информационно-коммуникационных технологий, но допускает значительные ошибки.	устранения угроз информационной безопасности; эксплуатации современного электронного оборудования и информационно-коммуникационных технологий	выявления и устранения угроз информационной безопасности; эксплуатации современного электронного оборудования и информационно-коммуникационных технологий

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:
от 45 до 59 баллов – «удовлетворительно»;
от 60 до 79 баллов – «хорошо»;
от 80 баллов – «отлично».

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

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
1 этап Знания	Знать базовые экономические понятия (спрос, предложение, цена, стоимость, товар, деньги, доходы, расходы, прибыль, риск, собственность, управление, рынок, фирма, государство)	ОК-2. Способность использовать основы экономических знаний в различных сферах деятельности	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Знать средства контроля контента, средства анализа защищенности и средства обнаружения атак, средства защиты от несанкционированного доступа	ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их	Практическое задание, Письменная контрольная работа, Лабораторная

		реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	работа
	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности, возможности и особенности организационных средств безопасности и защиты информации, состояние законодательной базы и стандарты в области информационной безопасности	ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Знать правовые основы организации защиты государственной тайны и конфиденциальной информации	ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Знать понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Знать общеметодологические принципы теории информационной безопасности	ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации, нормативные методические документы Федеральной	ПК-15. Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с	Практическое задание, Письменная контрольная работа, Лабораторная

	службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	работа
2 этап Умения	Уметь решать типичные задачи, связанные с личным финансовым планированием (рассчитать процентные ставки, оценить целесообразность взятия кредита с точки зрения текущих и будущих доходов и расходов, оценить эффективность страхования)	ОК-2. Способность использовать основы экономических знаний в различных сферах деятельности	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Уметь использовать базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность	ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Уметь реализовывать на практике принципы политики безопасности, использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Уметь разрабатывать организационно-распорядительные документы по вопросам защиты информации	ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Уметь использовать методы количественного представления информации и основные закономерности ее	ПК-6. Способность принимать участие в организации и проведении контрольных проверок	Практическое задание, Письменная контрольная

	преобразования в каналах при выполнении комплекса мер по информационной безопасности	работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	работа, Лабораторная работа
	Уметь обосновывать организационно-технические мероприятия по защите информации.	ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Уметь анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности	ПК-15. Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Практическое задание, Письменная контрольная работа, Лабораторная работа
3 этап Владения навыками	Владеть методами личного финансового планирования (бюджетирование, оценка будущих доходов и расходов, сравнение условий различных финансовых продуктов, управление рисками, применение инструментов защиты прав потребителя финансовых услуг)	ОК-2. Способность использовать основы экономических знаний в различных сферах деятельности	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Владеть методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам	ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Владеть навыками	ПК-4. Способность	Практическое

	формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности	участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	задание, Письменная контрольная работа, Лабораторная работа
	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	ПК-5. Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Практическое задание, Письменная контрольная работа, Лабораторная работа
	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	ПК-6. Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Владеть навыками обоснования, выбора, реализации и контроля результатов управленческого решения	ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Владеть навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности, навыками обеспечения и соблюдения режима секретности	ПК-15. Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Практическое задание, Письменная контрольная работа, Лабораторная работа

4.3. Рейтинг-план дисциплины

Рейтинг-план дисциплины представлен в приложении 2.

Экзамен

Структура экзаменационного билета

Экзаменационный билет состоит из двух вопросов

Типовые экзаменационные материалы

Вопросы к экзамену 6 семестр

1. Сущность и задачи комплексной защиты информации
2. Понятийный аппарат в области обеспечения безопасности информации
3. Цели, задачи и принципы построения КСЗИ
4. О понятиях безопасности и защищенности
5. Разумная достаточность и экономическая эффективность
6. Управление безопасностью предприятия. Международные стандарты
7. Цели и задачи защиты информации в автоматизированных системах
8. Современное понимание методологии защиты информации
9. Особенности национального технического регулирования
10. Что понимается под безопасностью ИТ?
11. Документы пользователя
12. Требования к средствам обеспечения безопасности
13. Принципы организации и этапы разработки КСЗИ
14. Методологические основы организации КСЗИ
15. Разработка политики безопасности и регламента безопасности предприятия
16. Система управления информационной безопасностью предприятия.
17. Принципы построения и взаимодействие с другими подразделениями 46
18. Требования, предъявляемые к КСЗИ
19. Этапы разработки КСЗИ
20. Факторы, влияющие на организацию КСЗИ
21. Влияние формы собственности на особенности защиты информации ограниченного доступа
22. Влияние организационно-правовой формы предприятия на особенности защиты информации ограниченного доступа
23. Характер основной деятельности предприятия
24. Состав, объекты и степень конфиденциальности защищаемой информации
25. Структура и территориальное расположение предприятия
26. Режим функционирования предприятия
27. Конструктивные особенности предприятия
28. Количественные и качественные показатели ресурсообеспечения
29. Степень автоматизации основных процедур обработки защищаемой информации
30. Определение и нормативное закрепление состава защищаемой информации
31. Классификация информации по видам тайны и степеням конфиденциальности
32. Нормативно-правовые аспекты определения состава защищаемой информации
33. Определение состава защищаемой информации, отнесенной к коммерческой тайне предприятия
34. Методика определения состава защищаемой информации

35. Порядок внедрения перечня сведений, составляющих КТ, внесение в него изменений и дополнений
36. Определение объектов защиты

Вопросы к экзамену 7 семестр

37. Методика выявления состава носителей защищаемой информации
38. Особенности взаимоотношений с контрагентами как объект защиты информации ограниченного доступа
39. Факторы, определяющие необходимость защиты периметра и здания предприятия
40. Особенности помещений как объектов защиты для работы по защите информации
41. Транспортные средства и особенности транспортировки
42. Состав средств обеспечения, подлежащих защите
43. Дестабилизирующие воздействия на информацию и их нейтрализация
44. Факторы, создающие угрозу информационной безопасности
45. Угрозы безопасности информации
46. Модели нарушителей безопасности АС
47. Подходы к оценке ущерба от нарушений ИБ
48. Обеспечение безопасности информации в непредвиденных ситуациях
49. Реагирование на инциденты ИБ
50. Резервирование информации и отказоустойчивость
51. Определение потенциальных каналов и методов несанкционированного доступа к информации
52. Задачи КСЗИ по выявлению угроз и КУИ
53. Особенности защиты речевой информации
54. Определение возможностей несанкционированного доступа к защищаемой информации
55. Методы и способы защиты информации
56. Классификация СЗИ НСД
57. Механизмы обеспечения безопасности информации
58. Разграничение доступа. Регистрация и аудит
59. Методика выявления нарушителей, тактики их действий и состава интересующей их информации
60. Определение компонентов КСЗИ
61. Методика синтеза СЗИ
62. Проектирование системы защиты информации для существующей АС
63. Определение условий функционирования КСЗИ
64. Содержание концепции построения КСЗИ
65. Объекты защиты. Цели и задачи обеспечения безопасности информации
66. Основные положения технической политики в области обеспечения безопасности информации АС организации
67. Основные принципы построения КСЗИ
68. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов
69. Первоочередные мероприятия по обеспечению безопасности информации АС организации
70. Разработка модели КСЗИ
71. Общая характеристика задач моделирования КСЗИ
72. Формальные модели безопасности и их анализ

73. Классификация формальных моделей безопасности
74. Модели обеспечения конфиденциальности
75. Модели обеспечения целостности
76. Субъектно-ориентированная модель
77. Прикладные модели защиты информации в АС
78. Формальное построение модели защиты
79. Описание объекта защиты
80. Декомпозиция АС на субъекты и объекты
81. Модель безопасности: неформальное описание
82. Декомпозиция системы защиты информации
83. Противостояние угрозам. Реализация системы защиты информации субъекта АС субъектно-объектной модели
84. Формализация модели безопасности
85. Процедура создания пары субъект-объект, наделение их атрибутами безопасности
86. Осуществление доступа субъекта к объекту.
87. Технологическое и организационное построение КСЗИ
88. Характеристика основных стадий создания КСЗИ
89. Назначение и структура технического задания (общие требования к содержанию)
90. Предпроектное обследование, технический проект, рабочий проект. Апробация и ввод в эксплуатацию
91. Кадровое обеспечение функционирования комплексной системы защиты информации
92. . Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа
93. Подбор и обучение персонала
94. Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации
95. Перечень вопросов ЗИ, требующих документационного закрепления
96. Назначение, структура и содержание управления КСЗИ
97. Принципы и методы планирования функционирования КСЗИ. Сущность и содержание контроля функционирования
98. Проведение контрольных мероприятий в КСЗИ
99. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций. Технология принятия решений в условиях ЧС.
100. Факторы, влияющие на принятие решений в условиях ЧС. Подготовка мероприятий на случай возникновения ЧС
101. Общая характеристика подходов к оценке эффективности КСЗИ. Методы и модели оценки эффективности КСЗИ
102. Показатель уровня защищенности, основанный на экспертных оценках. Методы проведения экспертного опроса
103. Экономический подход к оценке эффективности КСЗИ

Пример экзаменационного билета

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Направление подготовки
10.03.01 Информационная безопасность

Комплексная система защиты информации на предприятии

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1

1. *Методика выявления состава носителей защищаемой информации*

2. *Общая характеристика задач моделирования КСЗИ*

Зав. кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Направление подготовки
10.03.01 Информационная безопасность

Комплексная система защиты информации на предприятии

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №2

1. *Особенности взаимоотношений с контрагентами как объект защиты информации ограниченного доступа*

2. *Формальные модели безопасности и их анализ*

Зав. кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

Перевод оценки из 100-балльной в четырехбалльную производится следующим образом:

- отлично - от 80 до 110 баллов (включая 10 поощрительных баллов);
- хорошо - от 60 до 79 баллов;
- удовлетворительно - от 45 до 59 баллов;
- неудовлетворительно - менее 45 баллов.

Критерии оценивания ответа на экзамене

Критерии оценки (в баллах):

- **25-30** ***баллов*** выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов. Студент без затруднений ответил на все дополнительные вопросы
- **17-24** ***баллов*** выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности
- **10-16** баллов выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос.
- **1-10** ***баллов*** выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических. Студент не смог ответить ни на один дополнительный вопрос.

Примерная тематика курсовых проектов

1. Разработка политики безопасности и регламента безопасности предприятия
2. Система управления информационной безопасностью предприятия.
3. Этапы разработки КСЗИ
4. Влияние формы собственности на особенности защиты информации ограниченного доступа
5. Влияние организационно-правовой формы предприятия на особенности защиты информации ограниченного доступа
6. Порядок внедрения Перечня сведений, составляющих КТ, внесение в него изменений и дополнений
7. Подходы к оценке ущерба от нарушений ИБ
8. Обеспечение безопасности информации в непредвиденных ситуациях
9. Реагирование на инциденты ИБ
10. Задачи КСЗИ по выявлению угроз и КУИ
11. Методика выявления нарушителей, тактики их действий и состава интересующей их информации
12. . Определение компонентов КСЗИ
13. Основные принципы построения КСЗИ
14. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов
15. Первоочередные мероприятия по обеспечению безопасности информации АС организации
16. Разработка модели КСЗИ
17. Технологическое и организационное построение КСЗИ
18. Кадровое обеспечение функционирования комплексной системы защиты
19. Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации
20. Перечень вопросов ЗИ, требующих документационного закрепления
21. Проведение контрольных мероприятий в КСЗИ

22. Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций
23. Технология принятия решений в условиях ЧС
24. Подготовка мероприятий на случай возникновения ЧС
25. Принципы построения и функционирования аппаратных и антивирусных систем
26. Современные межсетевые экраны и особенности их применения
27. Адаптивное управление информационной безопасностью АС при угрозах реализации атаки на сервер организации
28. Методы обеспечения информационной безопасности при реализации угрозы попытки доступа
29. Оценка информационных рисков объекта информатизации и ее влияние на систему защиты информации
30. Проектирование системы защиты информации объекта информатизации на конкретном примере
31. Основные угрозы безопасности информации по электрическому и электромагнитному каналу утечки информации
32. Анализ информационно-аналитического обеспечения работы руководителя подразделения защиты информации
33. Алгоритм верификации личности и их применение в системе защиты информации
34. Математическое моделирование информационных конфликтов

Критерии оценивания курсового проекта

Оценка «отлично»:

работа выполнена в полном объеме и изложена грамотным языком в определенной логической последовательности с точным использованием специализированной терминологии; показано уверенное владение прикладными программами.

Оценка «хорошо»:

работа выполнена в полном объеме, но имеет один из недостатков: в работе допущены один-два недочета при освещении основного содержания ответа; нет определенной логической последовательности, неточно используется специализированная терминология;

Оценка «удовлетворительно»:

работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.

Комплект контрольных работ

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

Модуль 1

Сущность и задачи комплексной защиты информации

Письменная контрольная работа №1
Общие вопросы КСЗИ

Вопросы

1. Различные определения КСЗИ
2. Кому, для чего, когда нужна КСЗИ?
3. Кто разрабатывает, создает, эксплуатирует КСЗИ?

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	8
Выполнены пункты 1-3	15
Максимальный балл	15

Модуль 2
Разработка модели КСЗИ

Письменная контрольная работа №2
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 банка
3. Изучить их и подготовить краткий отчет.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	5
Выполнены пункты 1-3	7
Максимальный балл	7

Модуль 3
Назначение, структура и содержание управления КСЗИ

Письменная контрольная работа №3
Оценка и минимизация ущерба

Вопросы

1. Оценка ущерба от нарушителей ИБ.
2. Непредвиденные ситуации и обеспечение безопасности информации.
3. Реагирование на инциденты ИБ.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	8
Выполнены пункты 1-3	15
Максимальный балл	15

Модуль 4
Общая характеристика подходов к оценке эффективности КСЗИ
Письменная контрольная работа №4
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	5
Выполнены пункты 1-3	7
Максимальный балл	7

Комплект практических заданий

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

Модуль 1

Сущность и задачи комплексной защиты информации

Типовое практическое 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 1-2	8
Выполнены пункты 1-3	14
Максимальный балл	14

Модуль 2

Разработка модели КСЗИ

Типовое практическое 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 1-2	8
Выполнены пункты 1-3	14
Максимальный балл	14

Модуль 3

Назначение, структура и содержание управления КСЗИ

Типовое практическое задание 3

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.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	8
Выполнены пункты 1-3	14
Максимальный балл	14

Методические указания

а. Изучить ГОСТ по написанию ТЗ и образцы готовых вариантов.
б. Помнить, для чего и для кого разрабатывается ТЗ.

Модуль 4

Общая характеристика подходов к оценке эффективности КСЗИ

Типовое практическое задание 4

Разработка перечня информации, составляющей коммерческую тайну организации

1. Выбрать (придумать гипотетическую) коммерческую организацию.
2. Изучить деятельность организации.
3. Составить перечень информации (всей), циркулирующей в организации.
4. Провести анализ перечня с фильтрацией информации, имеющей коммерческую ценность для организации.
5. Составить перечень информации, составляющей коммерческую тайну организации

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	8
Выполнены пункты 1-5	14
Максимальный балл	14

Комплект лабораторных работ

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

Модуль 2

Разработка модели КСЗИ

Типовая лабораторная работа 1
Правовая 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%	5
Выполнены пункты 100%	8
Максимальный балл	8

Модуль 4
Общая характеристика подходов к оценке эффективности КСЗИ

Типовая лабораторная работа 2
Оценка эффективности системы защиты информации

1. Для коммерческой организации из практической работы №4 разработать систему защиты информации.
3. Выбрать модели оценки экономической эффективности системы защиты.
4. Оценить экономическую эффективность разработанной системы защиты информации выбранной коммерческой организации.
5. Составить отчет по работе.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	5
Выполнены пункты 1-5	8
Максимальный балл	8

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. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356
2. Плашенков, В. Обеспечение безопасности бизнеса промышленных предприятий: теория и практика : учебное пособие / В. Плашенков ; науч. ред. А.Н. Зуев ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «ЧЕРЕПОВЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ», Институт информационных технологий. - Череповец : Издательство ЧГУ, 2014. - 331 с. : ил., табл. - Библиогр. в кн. - ISBN 978-5-85341-634-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=434840
3. Милославская, Н.Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса : учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва : Горячая линия - Телеком, 2013. - 170 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 3). - Библиогр. в кн. - ISBN 978-5-9912-0273-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253577

Дополнительная литература

4. 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
5. 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 — Загл. с экрана.
6. 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.
7. Семь безопасных информационных технологий [Электронный ресурс] : учебник / А.В. Барабанов [и др.] ; под ред. Маркова А.С.. — Электрон. дан. — Москва : ДМК Пресс, 2017. — 224 с. — Режим доступа: https://e.lanbook.com/book/97352. — Загл. с экрана.
8. 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. www.fstec.ru – сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России
7. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
9. www.newlibrary.ru – Новая электронная библиотека;
10. www. edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
15. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1. *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),	Лекции, практические занятия, курсовое проектирование, 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

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 курсового проектирования (выполнения курсовых работ):***аудитория №613 (гуманитарный корпус). **4. *учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **5. *учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416		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 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.

(гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **6.*помещения для самостоятельной работы:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус).		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

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Содержание рабочей программы
дисциплины
Комплексная система защиты информации на предприятии

на 6семестр - ОФО

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	33,2
лекций	16
практических / семинарских	16
лабораторных	-
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	1,2
Учебных часов на самостоятельную работу	76
Учебных часов на подготовку к экзамену	34,8

Форма контроля:
Экзамен 6 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)					Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
			ЛК	ПР / Сем	ЛР	СРС			
1	2		4	5	6	7	8	9	10
1	**Сущность и задачи комплексной защиты информации** Принципы организации и этапы разработки КСЗИ Факторы, влияющие на организацию КСЗИ Определение и нормативное закрепление состава защищаемой информации		2	2		9	1-3	Изучить вопросы определения несанкционированного доступа к защищаемой информации	Практическое задание, Письменная контрольная работа
2	Определение объектов защиты Дестабилизирующие воздействия на информацию и их нейтрализация		2	2		9	1-4	Изучить вопросы определения несанкционированного доступа к защищаемой информации	Практическое задание, Письменная контрольная работа, Лабораторная работа
3	Определение потенциальных каналов и методов		2	2		9	1-3	Изучить вопросы определения несанкционирова	Практическое задание, Письменная

	несанкционированного доступа к информации							нного доступа к защищаемой информации	контрольная работа, Лабораторная работа
4	Определение компонентов КСЗИ Определение условий функционирования КСЗИ		2	2		11	1-8	Изучить возможности несанкционированного доступа к защищаемой информации	Практическое задание, Письменная контрольная работа, Лабораторная работа
5	**Разработка модели КСЗИ** Технологическое и организационное построение КСЗИ		2	2		9	1-4	Изучить возможности несанкционированного доступа к защищаемой информации	Практическое задание, Письменная контрольная работа, Лабораторная работа
6	Кадровое обеспечение функционирования комплексной системы защиты информации		2	2		9	1-6	Изучить актуальные вопросы построения КСЗИ	Практическое задание, Письменная контрольная работа, Лабораторная работа
7	Материально-техническое обеспечение комплексной системы защиты информации		2	2		9	1-8	Изучить вопросы оправданности построения КСЗИ	Практическое задание, Письменная контрольная работа, Лабораторная работа
8	Нормативно-методическое		2	2		11	1-8	Изучить вопросы целесообразност	Практическое задание,

	обеспечение комплексной системы защиты информации							и построения КСЗИ	Письменная контрольная работа, Лабораторная работа
	Всего		16	16		76			

Комплексная система защиты информации на предприятии

на 7 семестр - ОФО

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	57,2
лекций	18
практических / семинарских	36
лабораторных	-
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	3,2
Учебных часов на самостоятельную работу	52
Учебных часов на подготовку к экзамену	34,8

Форма контроля:
Экзамен 7 семестр
В том числе: курсовой проект 7 семестр, контактных часов – 2. часов на самостоятельную работу – 20

№	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	**Назначение, структура и содержание управления КСЗИ** Принципы функционирования КСЗИ		2	4		8	1-4	Изучить принципы функционирования КСЗИ в штатном режиме функционирования	Практическое задание, Письменная контрольная работа, Лабораторная работа
2	Методы планирования функционирования КСЗИ		2	4		8	1-7	Изучить правовые аспекты защиты информации в штатном режиме функционирования	Практическое задание, Письменная контрольная работа
3	Сущность и содержание контроля функционирования		2	4		8	1-7	Изучить эффективность правовых аспектов защиты информации в условиях чрезвычайных ситуаций	Практическое задание, Письменная контрольная работа, Лабораторная работа

4	Управление комплексной системой защиты информации в условиях чрезвычайных ситуаций		2	6		10	1-7	Изучить правовые аспекты защиты информации в условиях чрезвычайных ситуаций	Практическое задание, Письменная контрольная работа, Лабораторная работа
5	**Общая характеристика подходов к оценке эффективности КСЗИ** Методы оценки эффективности КСЗИ		2	2		5	1-8	Сравнить отечественный и зарубежный опыт подходов к оценке эффективности КСЗИ	Практическое задание, Письменная контрольная работа
6	Модели оценки эффективности КСЗИ		2	4		5	1-8	Изучить отечественные модели оценки эффективности КСЗИ	Практическое задание, Письменная контрольная работа, Лабораторная работа
7	Показатель уровня защищенности, основанный на экспертных оценках		2	4		5	1-8	Изучить отечественный опыт подходов к оценке эффективности КСЗИ	Практическое задание, Письменная контрольная работа
8	Методы проведения экспертного опроса		2	4		5	1-8	Изучить зарубежный опыт подходов к оценке эффективности КСЗИ	Практическое задание, Письменная контрольная работа, Лабораторная

									работа
9	Экономический подход к оценке эффективности КСЗИ		2	4		6	1-8	Сравнить отечественный и зарубежный опыт подходов к оценке эффективности КСЗИ	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Всего		18	36		52	1-8		
	Курсовой проект						1-8	Курсовой проект по заданной теме	

Рейтинг – план дисциплины

Комплексная система защиты информации на предприятии

Направление подготовки 10.03.01 Информационная безопасность

Курс 3, семестр 6

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. **Сущность и задачи комплексной защиты информации**				
Текущий контроль				
1. Аудиторная работа	6	1	1	6
2. Практическая работа №1	14	1	0	14
Рубежный контроль				
1. Письменная контрольная работа №1	15	1	0	15
Всего				35
Модуль 2. **Разработка модели КСЗИ**				
Текущий контроль				
1. Аудиторная работа	6	1	1	6
2. Практическая работа №2	14	1	0	14
Рубежный контроль				
1. Письменная контрольная работа №2	7	1	0	7
2. Лабораторная работа №1	8	1	0	8
Всего				35
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Экзамен			0	30

Рейтинг – план дисциплины

Комплексная система защиты информации на предприятии

Направление подготовки 10.03.01 Информационная безопасность
Курс 4, семестр 7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 3. **Назначение, структура и содержание управления КСЗИ**				
Текущий контроль				
1. Аудиторная работа (участие в практических занятиях)	6	1	1	6
2. Практическая работа №3	14	1	0	14
Рубежный контроль				
1. Письменная контрольная работа №3	15	1	0	15
Всего				35
Модуль 4. **Общая характеристика подходов к оценке эффективности КСЗИ**				
Текущий контроль				
1. Аудиторная работа (участие в практических занятиях)	6	1	1	6
2. Практическая работа №4	14	1	0	14
Рубежный контроль				
1. Письменная контрольная работа №4	7	1	0	7
2 Лабораторная работа №2	8	1	0	8
Всего				35
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Экзамен			0	30