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

Утверждено:
на заседании кафедры
протокол № 11 от «20» июня 2019 г.
Зав. кафедрой / А.С. Исмагилова

Согласовано:
Председатель УМК института
/Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Организационное и правовое обеспечение информационной безопасности
Б1.Б.17 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: 2019 г.

Уфа 2019 г.

Составитель: доцент И.А. Шагапов

Рабочая программа дисциплины утверждена на заседании кафедры управления информационной безопасностью
Протокол № 11 от «20» июня 2019 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 4
2. Цель и место дисциплины в структуре образовательной программы 7
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)..... 7
4. Фонд оценочных средств по дисциплине 7
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 7
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..... 25
4.3. Рейтинг-план дисциплины..... 29
5. Учебно-методическое и информационное обеспечение дисциплины 41
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины 41
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины 41
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине 42

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 основы российской правовой системы и законодательства, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	ОПК-5. Способность использовать нормативные правовые акты в профессиональной 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 стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, методики анализа рисков информационных систем	ПК-7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.	
	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и	ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по	

	оптимизации, общеметодологические принципы теории информационной безопасности	обеспечению информационной безопасности, управлять процессом их реализации	
	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 предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	ОПК-5. Способность использовать нормативные правовые акты в профессиональной 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 интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных	ПК-7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.	
	Уметь реализовывать на практике принципы политики безопасности, использовать закономерности	ПК-13. Способность принимать участие в формировании, организовывать и поддерживать	

	преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
	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 опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	ОПК-5. Способность использовать нормативные правовые акты в профессиональной 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 интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	ПК-7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.	
	Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для	ПК-13. Способность принимать участие в формировании, организовывать и поддерживать	

	управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности	выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
	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 «Организационное и правовое обеспечение информационной безопасности» относится к обязательным дисциплинам базовой части.

Дисциплина изучается на 2 курсе в 3,4 семестрах.

Целью дисциплины «Организационное и правовое обеспечение информационной безопасности» является приобретение обучающимися знаний по организационному и правовому обеспечению защиты информации, а также формирование практических навыков работы в реальных условиях деятельности по защите информации.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «Информатика», «Основы информационной безопасности», «Информационные технологии».

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

ОПК-5. Способность использовать нормативные правовые акты в профессиональной деятельности

Этап (уровень) освоения компетенци	Планируемые результаты обучения (показатели	Критерии оценивания результатов обучения (зачет)	
		«Не зачтено»	«Зачтено»

и	достижения заданного уровня освоения компетенций)		
Первый этап (уровень)	Знать основы российской правовой системы и законодательства, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	Фрагментарные представления об основах российской правовой системы и законодательства, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	Сформированные представления об основах российской правовой системы и законодательства, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности
Второй этап (уровень)	Уметь предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	Фрагментарное умение предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	Сформированное умение предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности
Третий этап (уровень)	Владеть опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	Фрагментарное владение опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	Успешное и систематическое владение опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности

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 обучения (зачет)	
		«Незачтено»	«Зачтено»

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	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	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	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	Критерии оценивания результатов обучения (зачет)	
		«Незачтено»	«Зачтено»

	уровня освоения компетенций)		
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 законодательной базы и стандарты в области информационной безопасности	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 законодательной базы и стандарты в области информационной безопасности	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 законодательной базы и стандарты в области информационной безопасности
Второй этап (уровень)	Уметь реализовывать на практике принципы политики безопасности, использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	Не показывает сформированные умения реализовывать на практике принципы политики безопасности, использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности.	Уверенно умеет реализовывать на практике принципы политики безопасности, использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности

Третий этап (уровень)	Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности	Не владеет навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности	Уверенно владеет навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности

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

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения (зачет)	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	Знать правовые основы организации защиты государственной тайны и конфиденциальной информации	Фрагментарно 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	Уверенно умеет разрабатывать организационно-распорядительные документы по вопросам защиты информации
Третий этап (уровень)	Владеть навыками работы с нормативными правовыми актами и	Не владеет основными 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

	навыками лицензирования в области защиты информации		

ПК-7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения (зачет)	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	Знать стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, методики анализа рисков информационных систем	Фрагментарно знает стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, методики анализа рисков информационных систем	Уверенно знает стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, методики анализа рисков информационных систем
Второй этап (уровень)	Уметь интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных	Не показывает сформированные умения интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных	Уверенно умеет интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных
Третий этап (уровень)	Владеть навыками интерпретации и обобщения результатов,	Не владеет основными навыками интерпретации и обобщения результатов, формулирования	Уверенно владеет навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений

	формулирования рекомендаций и принятия решений	рекомендаций и принятия решений	

ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения (зачет)	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности	Фрагментарно знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности	Уверенно знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности
Второй этап (уровень)	Уметь реализовывать на практике принципы политики безопасности, использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной	Не показывает сформированные умения реализовывать на практике принципы политики безопасности, использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	Уверенно умеет реализовывать на практике принципы политики безопасности, использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности

	безопасности		
Третий этап (уровень)	Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности	Не владеет основными навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности	Уверенно владеет навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности

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 обучения (зачет)	
		«Не зачтено»	«Зачтено»
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	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	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

	экспортному контролю в данной области		
Второй этап (уровень)	Уметь анализировать и составлять основные 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	Не показывает сформированные умения анализировать и составлять основные 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	Уверенно умеет анализировать и составлять основные 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
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 нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности, навыками обеспечения и соблюдения режима секретности	Уверенно владеет навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности, навыками обеспечения и соблюдения режима секретности

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).

ОПК-5. Способность использовать нормативные правовые акты в профессиональной 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 основы российской правовой системы и законодательства, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	Фрагментарные представления об основах российской правовой системы и законодательства, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	Неполные представления об основах российской правовой системы и законодательства, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	Сформированные, но содержащие отдельные неточности об основах российской правовой системы и законодательства, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	Сформированные представления об основах российской правовой системы и законодательства, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности
Второй этап (уровень)	Уметь предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	Фрагментарное умение предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать	В целом успешное, но не систематическое умение предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной	В целом успешное, но содержащее отдельные пробелы предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной	Сформированное умение предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать

		их в своей деятельности	деятельности, и использовать их в своей деятельности	деятельности, и использовать их в своей деятельности	их в своей деятельности
Третий этап (уровень)	Владеть опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	Фрагментарное владение опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	В целом успешное, но не систематическое владение опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	В целом успешное, но содержащее отдельные пробелы владения опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	Успешное и систематическое владение опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности

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	Фрагментарно знает политики, стратегии и технологии информационной	В целом знает основные политики, стратегии и технологии информационной	Знает основные политики, стратегии и технологии информационной	Уверенно знает политики, стратегии и технологии информационной

	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	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	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	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	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
Второй этап (уровень)	Уметь реализовывать на практике принципы политики безопасности, использовать закономерности и преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	Не показывает сформированные умения реализовывать на практике принципы политики безопасности, использовать закономерности и преобразования данных в каналах при выполнении комплекса мер по информационной безопасности.	Умеет использовать некоторые методы реализовывать на практике принципы политики безопасности, использовать закономерности и преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	Уверенно использует большинство методов реализовывать на практике принципы политики безопасности, использовать закономерности и преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	Уверенно умеет реализовывать на практике принципы политики безопасности, использовать закономерности и преобразования данных в каналах при выполнении комплекса мер по информационной безопасности
Третий этап (уровень)	Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.)	Не владеет навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.)	Владеет основными навыками формирования комплекса мер (правила, процедуры, практические	Владеет основными навыками формирования комплекса мер (правила, процедуры, практические	Уверенно владеет навыками формирования комплекса мер (правила, процедуры, практические

	для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности	для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности	приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности	приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности	приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности

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

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов экзамена и защиты курсового проекта			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
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 лицензировани	Не владеет основными навыками работы с нормативными правовыми актами и навыками	Владеет основными навыками работы с нормативными правовыми актами и навыками	Владеет навыками работы с нормативными правовыми актами и навыками лицензирован	Уверенно владеет навыками работы с нормативными правовыми актами и навыками

	я в области защиты информации	лицензирование в области защиты информации	лицензирование в области защиты информации, но допускает значительные ошибки.	ия в области защиты информации	лицензирование в области защиты информации

ПК-7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.

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 стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, методики анализа рисков информационных систем	Фрагментарно знает стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, методики анализа рисков информационных систем	В целом знает стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, методики анализа рисков информационных систем	Знает основы стандартов построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, методики анализа рисков информационных систем	Уверенно знает стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, методики анализа рисков информационных систем
Второй этап (уровень)	Уметь интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных	Не показывает сформированные умения интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы	Умеет использовать некоторые методы интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике	Уверенно использует большинство методов интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике	Уверенно умеет интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки

		обработки данных	методы обработки данных	методы обработки данных	данных
Третий этап (уровень)	Владеть навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	Не владеет основными навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	Владеет основными навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений, но допускает значительные ошибки.	Владеет навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	Уверенно владеет навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений

ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

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	Фрагментарно знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности	В целом знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности	Знает основы политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности	Уверенно знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности

Второй этап (уровень)	Уметь реализовывать на практике принципы политики безопасности, использовать закономерности и преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	Не показывает сформированные умения реализовывать на практике принципы политики безопасности, использовать закономерности и преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	Умеет использовать некоторые методы реализации на практике принципы политики безопасности, использовать закономерности и преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	Уверенно использует большинство методов реализации на практике принципы политики безопасности, использовать закономерности и преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	Уверенно умеет реализовывать на практике принципы политики безопасности, использовать закономерности и преобразования данных в каналах при выполнении комплекса мер по информационной безопасности
Третий этап (уровень)	Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности	Не владеет основными навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности	Владеет основными навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности, но допускает значительные ошибки.	Владеет навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности	Уверенно владеет навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности

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	Критерии оценивания результатов экзамена и защиты курсового проекта			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)

	уровня освоения компетенций)				
Первый этап (уровень)	Знать основные нормативные и правовые акты в области информационн ой 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 информацион ной 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 информацион ной 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 информацион ной 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 информацион ной 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 оценку информации, используемых в профессиональ ной деятельности, ориентироватьс я в нормативно-правовых актах, регламентирую щих сферу профессиональ ной деятельности и использовать их в своей деятельности	Не показывает сформированн ые умения анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессионал ьной деятельности, ориентировать ся в нормативно-правовых актах, регламентиру ющих сферу профессионал ьной деятельности и использовать	Умеет использовать некоторые методы анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессионал ьной деятельности, ориентировать ся в нормативно-правовых актах, регламентиру ющих сферу профессионал ьной деятельности и	Уверенно использует большинство методов анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессионал ьной деятельности, ориентировать ся в нормативно-правовых актах, регламентиру ющих сферу профессионал ьной деятельности и	Уверенно умеет анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессионал ьной деятельности, ориентировать ся в нормативно-правовых актах, регламентиру ющих сферу профессионал ьной деятельности и использовать их в своей

		их в своей деятельности	использовать их в своей деятельности	использовать их в своей деятельности	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

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей дисциплины, перечисленных в рейтинг-плане дисциплины,
для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10.
Шкалы оценивания для экзамена:
от 45 до 59 баллов – «удовлетворительно»;
от 60 до 79 баллов – «хорошо»;
от 80 баллов – «отлично».

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

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
1 этап Знания	Знать основы российской правовой системы и законодательства, методы и средства правовой защиты интересов субъектов в	ОПК-5. Способность использовать нормативные правовые акты в профессиональной	Практическое задание, Письменная контрольная

	сфере информационной безопасности	деятельности	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 реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Практическое задание, Письменная контрольная работа, Лабораторная 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 стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, методики анализа рисков информационных систем	ПК-7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности	ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации, нормативные	ПК-15. Способность организовывать технологический процесс защиты информации	Практическое задание, Письменная контрольная

	методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	работа, Лабораторная работа
2 этап Умения	Уметь предвидеть юридические опасности и угрозы, связанные с использованием информации, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	ОПК-5. Способность использовать нормативные правовые акты в профессиональной 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 интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных	ПК-7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.	Практическое задание, Письменная контрольная работа, Лабораторная работа
	Уметь реализовывать на практике принципы политики безопасности, использовать закономерности преобразования данных в каналах	ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение	Практическое задание, Письменная контрольная

	при выполнении комплекса мер по информационной безопасности	комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	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 опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	ОПК-5. Способность использовать нормативные правовые акты в профессиональной 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 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	Практическое 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 интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	ПК-7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении	Практическое задание, Письменная контрольная работа, Лабораторная

		технико-экономического обоснования соответствующих проектных решений.	работа
	Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками выявления и устранения угроз информационной безопасности	ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	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.

Типовые вопросы для зачета

1. Концептуальные основы информационной безопасности
2. Основные принципы и условия организационной защиты информации.
3. Основные подходы и требования к организации системы защиты информации.
4. Основные силы и средства, используемые для организации защиты информации
5. Отнесение сведений к различным видам конфиденциальной информации.
6. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну.
7. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну
8. Отнесение сведений к государственной тайне.
9. Засекречивание сведений и их носителей
10. Отнесение сведений к коммерческой тайне.
11. Основания и порядок рассекречивания сведений и их носителей.
12. Основные положения допуска персонала предприятия к конфиденциальной информации.
13. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска.
14. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска.
15. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну
16. Порядок доступа к конфиденциальной информации командированных лиц

17. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации
18. Роль и место внутриобъектового режима в общей системе защиты информации на предприятии.
19. Основные цели, подходы и принципы организации внутриобъектового режима.
20. Силы и средства, используемые при организации внутриобъектового режима
21. Роль и место пропускного режима в общей системе защиты информации на предприятии.
22. Цели и задачи пропускного режима.
23. Основные элементы системы организации пропускного режима, используемые силы и средства
24. Организация охраны предприятий.

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).

Экзамен

Структура экзаменационного билета
Экзаменационный билет состоит из двух вопросов

Типовые экзаменационные материалы
Вопросы к экзамену

1. Основные принципы и условия организационной защиты информации.
2. Основные подходы и требования к организации системы защиты информации.
3. Основные силы и средства, используемые для организации защиты информации
4. Отнесение сведений к различным видам конфиденциальной информации.
5. Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну.
6. Грифы секретности и реквизиты носителей сведений, составляющих коммерческую тайну
7. Отнесение сведений к государственной тайне.
8. Засекречивание сведений и их носителей
9. Отнесение сведений к коммерческой тайне.
10. Основания и порядок рассекречивания сведений и их носителей.
11. Основные положения допуска персонала предприятия к конфиденциальной информации.
12. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне и условия прекращения допуска.
13. Порядок оформления и переоформления допуска к государственной тайне. Формы допуска.
14. Организация доступа персонала предприятия к сведениям, составляющим государственную тайну
15. Порядок доступа к конфиденциальной информации командированных лиц

16. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации
17. Роль и место внутриобъектового режима в общей системе защиты информации на предприятии.
18. Основные цели, подходы и принципы организации внутриобъектового режима.
19. Силы и средства, используемые при организации внутриобъектового режима
20. Роль и место пропускного режима в общей системе защиты информации на предприятии.
21. Цели и задачи пропускного режима.
22. Основные элементы системы организации пропускного режима, используемые силы и средства
23. Организация охраны предприятий
24. Организация защиты информации при проведении совещаний.
25. Порядок проведения совещания и использования его материалов
26. Организация защиты информации в ходе издательской и рекламной деятельности.
27. Основы организации защиты информации в ходе взаимодействия со средствами массовой информации
28. Основы защиты информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу.
29. Порядок передачи различных видов конфиденциальной информации иностранным государствам при осуществлении международного сотрудничества.
30. Ограничения прав гражданина, осведомленного в сведениях, составляющих государственную тайну, на выезд за границу.
31. Работа должностных лиц предприятия по оформлению документов на выезд сотрудников в служебные командировки и по частным делам
32. Допуск предприятий к проведению работ с конфиденциальной информацией.
33. Основные положения лицензирования деятельности предприятий, связанной с использованием сведений, составляющих государственную тайну.
34. Алгоритм работы лицензирующего органа по лицензированию деятельности предприятий
35. Допуск предприятий к проведению работ с конфиденциальной информацией.
36. Организация проведения государственной аттестации руководителей предприятий
37. Организация аналитической работы и контроля состояния защиты конфиденциальной информации
38. Организация и проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений
39. Уголовно-правовая защита сведений, составляющих коммерческую, налоговую или банковскую тайну
40. Уголовно-правовая защита в сфере компьютерной информации
41. Уголовно-правовая защита сведений, составляющих государственную тайну
42. Административно-правовая защита информации с ограниченным доступом
43. Гражданско-правовая защита служебной и коммерческой тайны
44. Дисциплинарная ответственность за разглашение и (или) утрату конфиденциальных сведений
45. Материальная ответственность за разглашение и (или) утрату конфиденциальных сведений

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

Организационное и правовое обеспечение информационной безопасности

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1

1. Основания и порядок рассекречивания сведений и их носителей.
2. Организация защиты информации в ходе издательской и рекламной деятельности.

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

Организационное и правовое обеспечение информационной безопасности

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №2

1. Концептуальные основы информационной безопасности
2. Уголовно-правовая защита сведений, составляющих государственную тайну

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 знаний. Студент не смог ответить ни на один дополнительный вопрос.

Примерная тематика курсовых проектов по дисциплине

1. Авторское право в интернет-эпоху
2. Административная ответственность как средство обеспечения информационной безопасности.
3. Анализ уязвимостей в области технической защиты информации
4. Аттестация объектов информатизации по требованиям безопасности
5. Вопросы правового обеспечения информационной безопасности в среде Интернет.
6. Государственное регулирование вопросов использования криптографических средств и электронной цифровой подписи.
7. Документация при организации внутриобъектового режима на предприятии.
8. Документация при организации пропускного режима на предприятии.
9. Защита прав, свобод и законных интересов в сфере обеспечения информационной безопасности.
10. Инсайдерская информация: методы борьбы в России и за рубежом.
11. Институт правовой защиты изобретений, полезных моделей, промышленных образцов
12. Институт правовой охраны программ для ЭВМ и баз данных
13. Информационная война в современных условиях
14. Информационные реестры: дилемма безопасности и доступности.
15. Лицензирование в области информационной безопасности.
16. Международное законодательство в области защиты информации.
17. Место органов ФСБ в системе обеспечения информационной безопасности.
18. Методы выявления нарушителей, тактики их действий и состава интересующей их информации
19. Модели нарушителя информационной безопасности
20. Модели угроз информационной безопасности
21. Мониторинг и анализ данных социальных сетей

22. Направления и виды разведывательной деятельности
23. Неправомерный доступ к компьютерной информации в сетях ЭВМ
24. Обеспечение безопасности критической информационной инфраструктуры
25. Обеспечение информационной безопасности в системе государственной службы.
26. Организационное обеспечение информационной безопасности при проведении закрытых мероприятий.
27. Организационно-правовые вопросы инженерно-технической защиты информации
28. Организационно-правовые вопросы применения полиграфа
29. Организационно-правовые вопросы программно-аппаратной защиты информации
30. Организационно-правовые основы обеспечения информационной безопасности органов государственной власти.
31. Организация внутриобъектового режима.
32. Организация и обеспечение режима секретности на объекте.
33. Организация режима коммерческой тайны предприятия
34. Организация службы информационной безопасности.
35. Основные документы, разрабатываемые на охраняемых объектах.
36. Особенности аудита информационной безопасности
37. Особенности защиты персональных данных
38. Особенности защиты служебной тайны
39. Особенности защиты государственной тайны
40. Особенности защиты информации при проведении конфиденциальных переговоров
41. Особенности защиты коммерческой тайны предприятия
42. Особенности защиты профессиональной тайны
43. Особенности информационных правоотношений, возникающих при производстве, передаче и распространении персональных данных.
44. Особенности обеспечения безопасности Интернета вещей
45. Ответственность при разглашении информации, составляющей коммерческую тайну предприятия
46. Подбор сотрудников и работа с кадрами на предприятии.
47. Подходы к оценке ущерба от нарушений ИБ
48. Правовое регулирование использования электронных документов в Российской Федерации
49. Разработка комплекта документов при проведении аттестационных испытаний защищаемых объектов.
50. Сертификация в области информационной безопасности.
51. Система информационной безопасности предприятия.
52. Совет Безопасности Российской Федерации: правовой статус и положение в системе государственных органов.
53. Современные киберугрозы: способы и методы борьбы.
54. Технические средства охраны источников информации
55. Технологии защищенного документооборота предприятия
56. Управление персоналом, допущенным к конфиденциальной информации
57. Управление рисками информационной безопасности
58. Утечка информации: понятие, виды и организационно-правовые способы борьбы с нею.
59. Уязвимости и угрозы информационной безопасности в области организационной защиты информации
60. Физическая защита информации

61. ФСТЭК в системе обеспечения информационной безопасности.
62. Экономическая эффективность защиты информации

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

Основы организационной защиты информации

Письменная контрольная работа №1

Основные силы и средства организации по ЗИ

Вопросы

1. С какой целью создается самостоятельное подразделение по защите информации в организации? Примеры.
2. Что означает аутсорсинг в области информационной безопасности? Примеры.
3. Обязанности руководителя организации в области защиты информации.

Критерии оценки

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

Модуль 2

Организация защиты информации на предприятии

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	6
Выполнены пункты 1-3	10
Максимальный балл	10

Модуль 3

Организация аналитической работы по защите конфиденциальной информации

Письменная контрольная работа №3

Отнесение сведений к конфиденциальной информации

Вопросы

1. Организационное обеспечение информационной безопасности при проведении закрытых мероприятий.
2. Разработка комплекта документов при организации пропускного режима на предприятии.
3. Основные документы, разрабатываемые на охраняемых объектах.

Критерии оценки

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

Модуль 4

Правовая защита конфиденциальной информации

Письменная контрольная работа№4

Работа с персоналом, допущенным к конфиденциальной информации

Вопросы

1. Права и обязанности оператора персональных данных.
2. Правовые основания работы с персональными данными.
3. Права субъекта персональных данных.
4. Права и обязанности держателя (обладателя) массивов персональных данных.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	3
Выполнены пункты 1-4	5
Максимальный балл	5

Комплект практических заданий

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

Модуль 1

Основы организационной 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	10
Выполнены пункты 1-3	15
Максимальный балл	15

Модуль 2

Организация защиты информации на предприятии

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	10
Выполнены пункты 1-3	15
Максимальный балл	15

Модуль 3

Организация аналитической работы по защите конфиденциальной информации

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

Правовая защита конфиденциальной информации

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 умений предусмотрены несколько лабораторных работ.

Модуль 1

Основы организационной защиты информации

Типовая лабораторная работа №1

Информационная безопасность технической системы

Цель работы: закрепление на практике понятия информационная безопасность технической системы

1. Выбрать произвольным образом техническую систему.
2. Привести подробное описание данной технической системы.
3. Расписать максимально подробно, что означает информационная безопасность для данной технической системы. Подобрать типичные примеры, аналогии.
4. Составить отчет по работе.

Методические рекомендации по выполнению работы.

Перед выполнением работы полезно ответить на следующие вопросы:

- Какие сложности возникли при описании технической системы?
- Чем отличается информационная безопасность технической системы от информационной безопасности личности?
- Чем отличается информационная безопасность от защиты информации?:

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	10
Выполнены пункты 1-4	15
Максимальный балл	15

Модуль 2

Организация защиты информации на предприятии

Типовая лабораторная работа №2

Информационная война и информационное оружие

Цель работы: закрепление на практике понятия информационная война

1. Группа делится на две подгруппы..
2. Выбирается область (вид) деятельности.
3. Каждая подгруппа выбирает тип «информационного оружия» и разрабатывает план «информационной войны» против другой подгруппы и пытается ее «реализовать», одновременно «защищаясь» от противника.
4. По результатам проводится анализ и «эффективность» действий каждой стороны.
5. Составить отчет по работе каждой подгруппы.

Методические рекомендации по выполнению работы.

При выполнении работы полезно ответить на следующие вопросы:

- Чем руководствовались при выборе информационного оружия?
- Какие методы защиты от информационного оружия противника применялись?
- Что означает эффективность применения информационного оружия?

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	10
Выполнены пункты 1-5	15
Максимальный балл	15

Модуль 3

Организация аналитической работы по защите конфиденциальной информации

Типовая лабораторная работа №3

Объекты и угрозы информационной безопасности

Цель работы: закрепление умений распознавать на практике угрозы объектам информационной безопасности

1. Выбрать произвольным образом объект обеспечения информационной безопасности.
2. Привести подробное описание объекта.
3. Составить перечень угроз объекту. Произвести классификацию по выбранному признаку.
4. Оценить актуальность этих угроз. Попытаться определить источники этих угроз. Насколько возможно, выявленные угрозы связать с уязвимостями объектов.
5. Составить отчет по работе.

Методические рекомендации по выполнению работы.

При выполнении работы полезно ответить на следующие вопросы:

- Чем руководствовались при составлении перечня угроз?
- Какие преимущества и недостатки имеет выбранная классификация угроз?
- Какова связь между угрозами и уязвимостями?

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	5
Выполнены пункты 1-5	10
Максимальный балл	10

Модуль 4

Правовая защита конфиденциальной информации

Типовая лабораторная работа №4

Обеспечение информационной безопасности объекта

Цель работы: закрепление умений обеспечивать информационную безопасность объекта

1. Для объекта из лабораторной работы №3 составить несколько вариантов для противодействия выявленным угрозам .
2. оценить эффективность каждого варианта.
3. Выбрать наиболее эффективный вариант.
4. Подробно расписать, как можно реализовать выбранный вариант противодействия угрозам.
5. Составить отчет по работе.

Методические рекомендации по выполнению работы.

При выполнении работы полезно ответить на следующие вопросы:

- На сколько типичным является объект?
- Из каких соображений были составлены варианты противодействия угрозам?
- На сколько «законным» является наиболее эффективный вариант?
- Что можно сказать, на счет экономической эффективности выбранного варианта?

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	5
Выполнены пункты 1-5	10
Максимальный балл	10

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557
2. Малюк, А.А. Теория защиты информации / А.А. Малюк. - Москва : Горячая линия - Телеком, 2012. - 184 с. : ил. - Библиогр. в кн. - ISBN 978-5-9912-0246-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253553
3. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. - 222 с. : ил. - Библиогр.: с. 214-215. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458204

Дополнительная литература

4. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93245
5. Малюк, А.А. Защита информации в информационном обществе : учебное пособие / А.А. Малюк. - Москва : Горячая линия-Телеком, 2015. - 229 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0481-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457170
6. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности : учебное пособие / Ю.И. Коваленко. - Москва : Горячая линия - Телеком, 2012. - 140 с. : ил. - Библиогр. в кн. - ISBN 978-5-9912-0261-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253538
7. Шишкин, В.В. МЕТОДИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. [Электронный ресурс] / В.В. Шишкин, Н.К. Юрков, Н.Ж. Мусин. — Электрон. дан. // Надежность и качество сложных систем. — 2013. — № 4. — С. 9-13. — Режим доступа: http://e.lanbook.com/journal/issue/298784 — Загл. с экрана.
8. 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.

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), аудитория № 516 (гуманитарный корпус). **2. *учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус),	Лекции, практические занятия, курсовое проектирование (выполнение курсовых работ), групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST - 1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) - 6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран	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

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 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус),		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**	централизованного тестирования БашГУ (Moodle).GNU General Public License..

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).		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.	

Приложение 1

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

Содержание рабочей программы дисциплины
Организационное и правовое обеспечение информационной безопасности
на 3 семестр

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	54,2
лекций	18
практических / семинарских	36
лабораторных	-
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	0,2
Учебных часов на самостоятельную работу	89,8
Учебных часов на подготовку к зачету	

Форма контроля:
Зачет 3 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	**Основы организационной защиты информации** Концептуальные основы информационной безопасности Организационные основы защиты информации		2	2		12	1-3	Изучить литературу по организацию допуска персонала к конфиденциальной информации	Письменная контрольная работа, Практическая работа, Лабораторная работа
2	Отнесение сведений к конфиденциальной информации.		2	4		8	1-3	Изучить нормативно-правовую базу по организацию допуска персонала к конфиденциальной информации	Письменная контрольная работа, Практическая работа, Лабораторная работа
3	Засекречивание и рассекречивание сведений		2	4		8	1-4	Изучить нормативно-правовую базу по	Письменная контрольная работа, Практическая

								засекречиванию и рассекречиванию сведений	работа, Лабораторная работа
4	Организация допуска и доступа персонала к конфиденциальной информации		2	4		8	1-5	Изучить нормативно-правовую базу по организацию допуска персонала к конфиденциальной информации	Письменная контрольная работа, Практическая работа, Лабораторная работа
5	Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации		2	4		8	1-5	Изучить нормативно-правовую базу по организацию допуска персонала к конфиденциальной информации	Письменная контрольная работа, Практическая работа, Лабораторная работа
6	**Организация защиты информации на предприятии** Организация внутриобъектового и пропускного режимов на предприятии Организация охраны предприятий		2	4		12,8	1-6	Собрать информацию для Положения о конфиденциальной информации для выбранного предприятия.	Письменная контрольная работа, Практическая работа, Лабораторная работа
7	Организация защиты информации при проведении совещаний, в ходе издательской и		2	6		11	1-8	Анализ собранной информации для Положения о конфиденциальн	Письменная контрольная работа, Практическая работа,

	рекламной деятельности							ой информации для выбранного предприятия.	Лабораторная работа
8	Основы защиты информации при осуществлении международного сотрудничества и выезде персонала предприятия за границу		2	4		11	1-7	Разработать структуру Положения о конфиденциальной информации для выбранного предприятия.	Письменная контрольная работа, Практическая работа, Лабораторная работа
9	Допуск предприятий к проведению работ с конфиденциальной информацией		2	4		10,8	1-8	Разработать Положение о конфиденциальной информации для выбранного предприятия.	Письменная контрольная работа, Практическая работа, Лабораторная работа
	Итого		18	36		89,8			

Организационное и правовое обеспечение информационной безопасности
на 4 семестр

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	35,2
лекций	16
практических / семинарских	16
лабораторных	-
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	3,2
Учебных часов на самостоятельную работу	56
Учебных часов на подготовку к экзамену	52,8

Форма контроля:
Экзамен 4 семестр
В том числе: курсовой проект 4 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	**Организация аналитической работы по защите конфиденциальной информации** Организация аналитической работы по защите конфиденциальной информации		2	2		27	1-6	Изучить правовые аспекты аналитической работы по защите конфиденциальной информации	Письменная контрольная работа, Практическая работа, Лабораторная работа
2	Организация контроля состояния защиты конфиденциальной информации		2	2		7	1-6	Изучить организационные аспекты аналитической работы по защите конфиденциальной информации	Письменная контрольная работа, Практическая работа, Лабораторная работа
3	Организация служебного расследования в случае разглашения сведений		2	2		7	1-6	Особенности аналитической работы по защите	Письменная контрольная работа,

	конфиденциального характера или утраты носителей сведений							конфиденциальной информации	Практическая работа, Лабораторная работа
4	Проведение служебного расследования в случае разглашения сведений конфиденциального характера или утраты носителей сведений		2	2		6	1-6	Эффективность аналитической работы по защите конфиденциальной информации	Письменная контрольная работа, Практическая работа, Лабораторная работа
5	**Правовая защита конфиденциальной информации** Уголовно-правовая защита сведений, составляющих коммерческую тайну. Уголовно-правовая защита в сфере компьютерной информации Уголовно-правовая защита сведений, составляющих государственную тайну		2	2		7	1-7	Изучить уголовно-правовую защиту в области персональных данных	Письменная контрольная работа, Практическая работа, Лабораторная работа
6	Административно-правовая защита информации с ограниченным доступом Гражданско-правовая защита служебной и коммерческой тайны		2	2		7	1-8	Изучить гражданско-правовую защита защиту в области персональных данных	Письменная контрольная работа, Практическая работа, Лабораторная работа
7	Дисциплинарная ответственность за разглашение и (или) утрату конфиденциальных		2	2		7	1-8	Изучить дисциплинарную ответственность за разглашение и (или)	Письменная контрольная работа, Практическая

	сведений							утрату конфиденциальных сведений в области персональных данных	работа, Лабораторная работа
8	Материальная ответственность за разглашение и (или) утрату конфиденциальных сведений		2	2		7	1-8	Изучить материальную ответственность за разглашение и (или) утрату конфиденциальных сведений в области персональных данных	Письменная контрольная работа, Практическая работа, Лабораторная работа
	Итого		16	16		56			
5	**Курсовой проект**					20	1-15	Курсовой проект по заданной теме	

Приложение 2

Рейтинг – план дисциплины

Организационное и правовое обеспечение информационной безопасности

Направление подготовки 10.03.01 Информационная безопасность

Курс 2, семестр 3

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. **Основы организационной защиты информации**				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №1	15	1	0	15
Рубежный контроль				
1. Письменная контрольная работа №1	10	1	0	10
2 Лабораторная работа №1	15	1	0	15
Всего				50
Модуль 2. **Организация защиты информации на предприятии**				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №2	15	1	0	15
Рубежный контроль				
1. Письменная контрольная работа №2	10	1	0	10
2 Лабораторная работа №2	15	1	0	15
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				

Рейтинг – план дисциплины

Организационное и правовое обеспечение информационной безопасности

Направление подготовки 10.03.01 Информационная безопасность

Курс 2, семестр 4

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 3. **Организация аналитической работы по защите конфиденциальной информации**				
Текущий контроль				
1. Аудиторная работа	6	1	1	6
2. Практическая работа №3	14	1	0	14
Рубежный контроль				
1. Письменная контрольная работа №3	5	1	0	5
2 Лабораторная работа №3	10	1	0	10
Всего				35
Модуль 4. **Правовая защита конфиденциальной информации**				
Текущий контроль				
1. Аудиторная работа	6	1	1	6
2. Практическая работа №4	14	1	0	14
Рубежный контроль				
1. Письменная контрольная работа №4	5	1	0	5
2 Лабораторная работа №4	10	1	0	10
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