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

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

Согласовано:
Председатель УМК института
/Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность предприятия
Б1.В.1.06

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: 2020 г.

г. Уфа 2020 г.

Составитель: доцент И.А. Шагапов

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

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

Заведующий кафедрой ____________________/ _____________Ф.И.О/

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

Заведующий кафедрой ____________________/ _____________Ф.И.О/

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

Заведующий кафедрой ____________________/ _____________Ф.И.О/

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

Заведующий кафедрой ____________________/ _____________Ф.И.О/

Список документов и материалов

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

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

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	Знать: правила определения информационных ресурсов, подлежащих защите, угрозы безопасности информации	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: правила работы по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности	ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.	
	Знать: способы анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности предприятия	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: правила анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-10 способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной	

		безопасности	
	Знать: правила организации технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативными правовыми актами	ПК-15 способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами	
	Знать: правила разработки подсистемы управления информационной безопасностью предприятия	ПСК-1 способность участвовать в разработке подсистемы управления информационной безопасностью	
	Знать: правила разработки предложений по совершенствованию системы управления информационной безопасностью предприятия	ПСК-2 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью	
Умения	Уметь: участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	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: участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
	Уметь: проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования	ПК-7 способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных	

	соответствующих проектных решений	решений	
	Уметь: проводить анализ информационной безопасности предприятия на соответствие требованиям стандартов в области информационной безопасности	ПК-10 способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	
	Уметь: способность организовывать технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативными правовыми актами	ПК-15 способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами	
	Уметь: участвовать в разработке подсистемы управления информационной безопасностью предприятия	ПСК-1 способность участвовать в разработке подсистемы управления информационной безопасностью	
	Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью предприятия	ПСК-2 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью	
Владения навыками	Владеть: приемами работ по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	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: приемами работ по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта	ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта	

	защиты	защиты	
	Владеть: способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности предприятия и участвовать в проведении технико-экономического обоснования соответствующих проектных 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: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-10 способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	
	Владеть: способностью организовывать технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативными правовыми актами	ПК-15 способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами	
	Владеть: способностью участвовать в разработке подсистемы управления информационной безопасностью предприятия Владеть: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью предприятия	ПСК-1 способность участвовать в разработке подсистемы управления информационной безопасностью	

	Владеть: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью предприятия	ПСК-2 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью	

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность предприятия» относится к обязательным дисциплинам вариативной части.

Дисциплина изучается на 4 курсе в 8 семестре.

Цель дисциплины «Информационная безопасность предприятия» освоение методов по поддержанию режимов безопасности и конфиденциальности; определению положений, прав, обязанностей и ответственности должностных лиц по вопросам безопасности, а также по осуществлению представительских функций предприятия в данной области ее деятельности; изучение и освоение задач по обеспечению безопасности предприятия, анализ возможных мероприятий организационно-технического и правового характера, направленных на сохранность собственности.

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

Полученные знания, навыки и умения используются при прохождении преддипломной практики и в ходе выполнения выпускной квалификационной работы.

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

Содержание рабочей программы представлено в Приложении 1.

4. Фонд оценочных средств по дисциплине

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

ОПК-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			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: правила определения информационных ресурсов, подлежащих	Фрагментарные представления о правилах определения информацион	Неполные представления о правилах определения информационных ресурсов,	Сформированные, но содержащие отдельные пробелы о правилах	Сформированные представления о правилах определения информацион

	защите, угрозы безопасности информации	ных ресурсов, подлежащих защите, угрозы безопасности информации	подлежащих защите, угрозы безопасности информации	определения информационных ресурсов, подлежащих защите, угрозы безопасности информации	ных ресурсов, подлежащих защите, угрозы безопасности информации
Второй этап (уровень)	Уметь: определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации	Фрагментарное умение определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации	В целом успешное, но не систематическое умение определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации	В целом успешное, но содержащее отдельные пробелы определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации	Сформированное умение определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации
Третий этап (уровень)	Владеть: технологией определения информационных ресурсов, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Фрагментарное владение навыками технологией определения информационных ресурсов, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	В целом успешное, но не систематическое владение навыками технологией определения информационных ресурсов, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	В целом успешное, но содержащее отдельные пробелы владения навыками технологией определения информационных ресурсов, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Успешное и систематическое владение навыками технологией определения информационных ресурсов, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

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

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: правила работы по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности	Фрагментарно знает основные правила работы по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности	В целом знает основные правила работы по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности	Знает основные правила работы по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности	Уверенно знает основные правила работы по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности
Второй этап (уровень)	Уметь: участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Не показывает сформированные умения участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Умеет использовать некоторые приемы работ по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Уверенно использует большинство приемов работ по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Уверенно использует приемы работ по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
Третий этап (уровень)	Владеть: приемами работ по реализации политики информационной безопасности,	Не владеет основными методами работ по реализации политики информационной	Владеет основными методами работ по реализации политики информационной	Владеет основными приемами работ по реализации политики информационной	Уверенно владеет основными приемами работ по реализации политики информацион

	применять комплексный подход к обеспечению информационной безопасности объекта защиты	безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты информации	безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты, но допускает значительные ошибки.	безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	ной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

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			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: способы анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности предприятия	Фрагментарно знает основные способы анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности предприятия.	В целом знает основные способы анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности предприятия	Знает основные способы анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности предприятия	Уверенно знает основные способы анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности предприятия.
Второй этап (уровень)	Уметь: проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении	Не показывает сформированные умения проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Умеет использовать некоторые методы анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Уверенно использует большинство методов анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Уверенно использует методы анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать

	технико-экономического обоснования соответствующих проектных решений	и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	в проведении технико-экономического обоснования соответствующих проектных решений
Третий этап (уровень)	Владеть: способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности предприятия и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Не владеет способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности предприятия и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Владеет основными методами анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности предприятия и участвовать в проведении технико-экономического обоснования соответствующих проектных решений, но допускает значительные ошибки.	Владеет основными методами анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности предприятия и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Уверенно владеет способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности предприятия и участвовать в проведении технико-экономического обоснования соответствующих проектных решений

ПК-10 способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: правила анализа информационной безопасности	Фрагментарно знает основные правила анализа информацион	В целом знает основные правила анализа информацион ной	Знает основные правила анализа информацион ной	Уверенно знает основные правила анализа информацион

	объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.	безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.	безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.	ной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.
Второй этап (уровень)	Уметь: проводить анализ информационной безопасности предприятия на соответствие требованиям стандартов в области информационной безопасности	Не показывает сформированные умения проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Умеет использовать некоторые методы проведения анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Уверенно использует большинство методов проведения анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Уверенно использует методы проведения анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
Третий этап (уровень)	Владеть: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Не владеет основными методами проведения анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Владеет основными методами проведения анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, но допускает значительные ошибки.	Владеет способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Уверенно владеет способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

ПК-15 способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами

Этап (уровень) освоения	Планируемые результаты обучения	Критерии оценивания результатов обучения			
		2 («Не удовлетворите	3 («Удовлетвор	4 («Хорошо»)	5 («Отлично»)

компетенции	(показатели достижения заданного уровня освоения компетенций)	льно»)	ительно»)		
Первый этап (уровень)	Знать: правила организации технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативными правовыми актами	Фрагментарно знает основные правила организации технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативным и правовыми актами	В целом знает основные правила организации технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативным и правовыми актами	Знает основные правила организации технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативным и правовыми актами	Уверенно знает основные правила организации технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативным и правовыми актами
Второй этап (уровень)	Уметь: способность организовывать технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативными правовыми актами	Не показывает сформированные умения организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативным и правовыми актами	Умеет использовать некоторые методы организации технологический процесс защиты информации ограниченного доступа в соответствии с нормативным и правовыми актами	Уверенно использует большинство методов организации технологический процесс защиты информации ограниченного доступа в соответствии с нормативным и правовыми актами	Уверенно использует методы организации технологический процесс защиты информации ограниченного доступа в соответствии с нормативным и правовыми актами
Третий этап (уровень)	Владеть: способностью организовывать технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативными правовыми актами	Не владеет способностью организовывать технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативным и правовыми актами	Владеет основными методами организовывать технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативным и правовыми актами, но допускает значительные ошибки.	Владеет способностью организовывать технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативным и правовыми актами	Уверенно владеет способностью организовывать технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативным и правовыми актами

ПСК-1 способность участвовать в разработке подсистемы управления информационной безопасностью

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: правила разработки подсистемы управления информационной безопасностью предприятия	Фрагментарно знает основные правила разработки подсистемы управления информационной безопасностью предприятия	В целом знает основные правила разработки подсистемы управления информационной безопасностью предприятия	Знает основные правила разработки подсистемы управления информационной безопасностью предприятия	Уверенно знает основные правила разработки подсистемы управления информационной безопасностью предприятия
Второй этап (уровень)	Уметь: участвовать в разработке подсистемы управления информационной безопасностью предприятия	Не показывает сформированные умения участвовать в разработке подсистемы управления информационной безопасностью	Умеет участвовать в разработке некоторых подсистем управления информационной безопасностью	Уверенно участвует в разработке некоторых подсистем управления информационной безопасностью	Уверенно участвует в разработке подсистемы управления информационной безопасностью
Третий этап (уровень)	Владеть: способностью участвовать в разработке подсистемы управления информационной безопасностью предприятия	Не владеет способностью участвовать в разработке подсистемы управления информационной безопасностью	Владеет основными методами разработки подсистемы управления информационной безопасностью, но допускает значительные ошибки.	Владеет основными методами разработки подсистемы управления информационной безопасностью	Уверенно владеет способностью участвовать в разработке подсистемы управления информационной безопасностью

ПСК-2 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью

Этап (уровень)	Планируемые результаты	Критерии оценивания результатов обучения			
		2 («Не	3	4 («Хорошо»)	5 («Отлично»)

освоения компетенции	обучения (показатели достижения заданного уровня освоения компетенций)	удовлетворительно»)	(«Удовлетворительно»)		
Первый этап (уровень)	Знать: правила разработки предложений по совершенствованию системы управления информационной безопасностью предприятия	Фрагментарно знает основные правила разработки предложений по совершенствованию системы управления информационной безопасностью	В целом знает основные правила разработки предложений по совершенствованию системы управления информационной безопасностью	Знает основные правила разработки предложений по совершенствованию системы управления информационной безопасностью	Уверенно знает основные правила разработки предложений по совершенствованию системы управления информационной безопасностью
Второй этап (уровень)	Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью предприятия	Не показывает сформированные умения разрабатывать предложения по совершенствованию системы управления информационной безопасностью	Умеет использовать некоторые методы разработки предложений по совершенствованию системы управления информационной безопасностью	Уверенно использует большинство методов разработки предложений по совершенствованию системы управления информационной безопасностью	Уверенно использует методы разработки предложений по совершенствованию системы управления информационной безопасностью
Третий этап (уровень)	Владеть: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью предприятия	Не владеет способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью	Владеет основными методами разработки предложений по совершенствованию системы управления информационной безопасностью	Владеет основными методами разработки предложений по совершенствованию системы управления информационной безопасностью	Уверенно владеет способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для экзамена: текущий контроль

– максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10).

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

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

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
1-й этап Знания	Знать: правила определения информационных ресурсов, подлежащих защите, угрозы безопасности информации	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	Лабораторная работа, Письменная контрольная работа,
	Знать: правила работы по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности	ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.	Лабораторная работа, Письменная контрольная работа,
	Знать: способы анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности предприятия	ПК-7 способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих	Лабораторная работа, Письменная контрольная работа,

		проектных решений	
	Знать: правила анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-10 способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Лабораторная работа, Письменная контрольная работа,
	Знать: правила организации технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативными правовыми актами	ПК-15 способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами	Лабораторная работа, Письменная контрольная работа,
	Знать: правила разработки подсистемы управления информационной безопасностью предприятия	ПСК-1 способность участвовать в разработке подсистемы управления информационной безопасностью	Лабораторная работа, Письменная контрольная работа,
	Знать: правила разработки предложений по совершенствованию системы управления информационной безопасностью предприятия	ПСК-2 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью	Лабораторная работа, Письменная контрольная работа,
2-й этап Умения	Уметь: участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	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	Лабораторная работа, Письменная контрольная работа,
	Уметь: участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Лабораторная работа, Письменная контрольная работа,
	Уметь:	ПК-7 способность	Лабораторная работа,

	проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Письменная контрольная работа,
	Уметь: проводить анализ информационной безопасности предприятия на соответствие требованиям стандартов в области информационной безопасности	ПК-10 способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Лабораторная работа, Письменная контрольная работа, Экзамен
	Уметь: способность организовывать технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативными правовыми актами	ПК-15 способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами	Лабораторная работа, Письменная контрольная работа,
	Уметь: участвовать в разработке подсистемы управления информационной безопасностью предприятия	ПСК-1 способность участвовать в разработке подсистемы управления информационной безопасностью	Лабораторная работа, Письменная контрольная работа,
	Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью предприятия	ПСК-2 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью	Лабораторная работа, Письменная контрольная работа,
3-й этап Владения навыками	Владеть: приемами работ по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	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	Лабораторная работа, Письменная контрольная работа,

	Владеть: приемами работ по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Лабораторная работа, Письменная контрольная работа,
	Владеть: способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности предприятия и участвовать в проведении технико-экономического обоснования соответствующих проектных 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	Лабораторная работа, Письменная контрольная работа,
	Владеть: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-10 способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Лабораторная работа, Письменная контрольная работа,
	Владеть: способностью организовывать технологический процесс защиты информации ограниченного доступа предприятия в соответствии с нормативными правовыми актами	ПК-15 способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами	Лабораторная работа, Письменная контрольная работа,
	Владеть: способностью участвовать в разработке подсистемы управления информационной безопасностью предприятия Владеть: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью	ПСК-1 способность участвовать в разработке подсистемы управления информационной безопасностью	Лабораторная работа, Письменная контрольная работа,

	предприятия		
	Владеть: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью предприятия	ПСК-2 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью	Лабораторная работа, Письменная контрольная работа,

4.3. Рейтинг-план дисциплины

Рейтинг-план дисциплины представлен в приложении 2.

Экзамен

Структура экзаменационного билета

Экзаменационный билет состоит из двух вопросов

Типовые экзаменационные материалы

Вопросы к экзамену

1. Основные направления, принципы и условия организационной защиты информации на предприятии
2. Основные принципы организационной защиты информации
3. Основные подходы и требования к организации системы защиты информации
4. Основные методы, силы и средства, используемые для организации защиты информации
5. Организация службы безопасности предприятия
6. Функции, задачи и особенности службы безопасности объекта.
7. Принципы организации службы безопасности объекта.
8. Типовая структура службы безопасности
9. Права, обязанности и ответственность сотрудников службы безопасности
10. Способы и формы взаимодействия службы безопасности объекта с правоохранительными органами.
11. Организационная защита информации на предприятии
12. Подбор сотрудников и работа с кадрами. Работа с посетителями.
13. Организация внутриобъектового режима
14. Организация охраны объектов. Организация пропускного режима
15. Организация аналитической работы в области защиты информации на предприятии
16. Основные направления аналитической работы
17. Функции аналитического подразделения
18. Основные этапы аналитической работы
19. Содержание и основные виды аналитических отчетов
20. Классификация методов анализа информации
21. Контроль физического доступа
22. Модели нарушителей

23. Мотивы, финансовое обеспечение, уровень подготовки, техническое обеспечение, предварительная подготовка нарушителей
24. Классы нарушителей
25. Выявление и оценка основных видов угроз. Классификация угроз
26. Функции службы безопасности по защите коммерческой тайны
27. Организация системы защиты коммерческой тайны
28. Формальные модели безопасности и их анализ
29. Классификация формальных моделей безопасности
30. Модели обеспечения конфиденциальности
31. Модели обеспечения целостности
32. Субъектно-ориентированная модель
33. Прикладные модели защиты информации в АС
34. Формальное построение модели защиты
35. Описание объекта защиты
36. Декомпозиция АС на субъекты и объекты
37. Модель безопасности: неформальное описание
38. Декомпозиция системы защиты информации
39. Противостояние угрозам. Реализация системы защиты информации субъекта АС субъектно-объектной модели
40. Формализация модели безопасности
41. Процедура создания пары субъект-объект, наделение их атрибутами безопасности
42. Осуществление доступа субъекта к объекту.
43. Назначение и структура технического задания (общие требования к содержанию)
44. Предпроектное обследование, технический проект, рабочий проект.
45. Апробация и ввод в эксплуатацию проекта.
46. Кадровое обеспечение функционирования системы защиты информации предприятия.
47. . Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа
48. Подбор и обучение персонала
49. Материально-техническое и нормативно-методическое обеспечение системы защиты информации предприятия
50. Перечень вопросов ЗИ, требующих документационного закрепления
51. Принципы и методы планирования функционирования.
52. Сущность и содержание контроля функционирования. Проведение контрольных мероприятий.
53. Управление системой защиты информации предприятия в условиях чрезвычайных ситуаций.
54. Технология принятия решений в условиях ЧС. Факторы, влияющие на принятие решений в условиях ЧС.
55. Подготовка мероприятий на случай возникновения ЧС
56. Общая характеристика подходов к оценке эффективности информационной безопасности предприятия.
57. Методы и модели оценки эффективности.
58. Показатель уровня защищенности, основанный на экспертных оценках. Методы проведения экспертного опроса

59. Экономический подход к оценке эффективности информационной безопасности предприятия.
60. Защита информации при осуществлении рекламной и публикаторской деятельности

Пример экзаменационного билета

Федеральное государственное бюджетное образовательное учреждение высшего образования

«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт истории и государственного управления

Направление подготовки
10.03.01 Информационная безопасность

Информационная безопасность предприятия

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. *Основные направления, принципы и условия организационной защиты информации на предприятии*

2. *Модели обеспечения целостности*

Зав. кафедрой УИБ А.С. Исмагилова
Кафедра управления информационной безопасностью

Федеральное государственное бюджетное образовательное учреждение высшего образования

«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт истории и государственного управления

Направление подготовки
10.03.01 Информационная безопасность

Информационная безопасность предприятия

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. *Основные принципы организационной защиты информации*
2. *Субъектно-ориентированная модель*

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, умение применять теоретические знания. 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.

Комплект контрольных работ

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

Модуль 1.

Основные направления, принципы и условия организационной защиты информации на предприятии

Письменная контрольная работа №1

Служба безопасности предприятия

Вопросы

1. Организация службы безопасности предприятия
2. Функции, задачи и особенности службы безопасности объекта.
3. Принципы организации службы безопасности объекта.
4. Типовая структура службы безопасности
5. Права, обязанности и ответственность сотрудников службы безопасности

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	8
Выполнены пункты 1-5	15
Максимальный балл	15

Модуль 2.

Организация аналитической работы в области защиты информации на предприятии

Письменная контрольная работа №2

Защита информации в условиях чрезвычайных ситуаций.

Вопросы

1. Управление системой защиты информации предприятия в условиях чрезвычайных ситуаций.
2. Технология принятия решений в условиях ЧС. Факторы, влияющие на принятие решений в условиях ЧС.
3. Подготовка мероприятий на случай возникновения ЧС

Критерии оценки

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

Комплект практических заданий

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

Модуль 1.
Основные направления, принципы и условия организационной защиты информации на предприятии
Типовая лабораторная работа 1

Задание 1. Разработка положения о коммерческой тайне предприятия

1. Выбрать (придумать гипотетическую) коммерческое предприятие.
2. Изучить деятельность предприятия.
3. Составить перечень информации (всей), циркулирующей на предприятии.
4. Разработать положение о коммерческой тайне данного предприятия.

Критерии оценки

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

Модуль 2.
Организация аналитической работы в области защиты информации на предприятии
Типовая лабораторная работа 2

Задание 2. Разработка технического задания (ТЗ) на создание системы защиты информации предприятия.

1. Изучить деятельность выбранного (гипотетически придуманного) предприятия.
2. Собрать необходимую информацию по предприятию.
3. Составить техническое задание на создание системы защиты информации предприятия.

Методические указания

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

Критерии оценки

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

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. Аверченков, В.И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356
2. 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.

Дополнительная литература

3. Шагапов, И.А. Защита коммерческой тайны на предприятии [Электронный ресурс]: учебное пособие / И.А. Шагапов; Башкирский государственный университет. — Уфа: РИЦ БашГУ, 2018. — Электрон. версия печ. публикации. — Доступ возможен через Электронную библиотеку БашГУ. — <URL:https://elib.bashedu.ru/dl/corp/Shagapov_Zazchita komm tajny na predprijatii_up_2018.pdf>.
4. Плашенков, В. Обеспечение безопасности бизнеса промышленных предприятий: теория и практика : учебное пособие / В. Плашенков ; науч. ред. А.Н. Зуев ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «ЧЕРЕПОВЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ», Институт информационных технологий. - Череповец : Издательство ЧГУ, 2014. - 331 с. : ил., табл. - Библиогр. в кн. - ISBN 978-5-85341-634-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=434840
5. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93245
6. Мирсанова, О.А. К ВОПРОСУ ОБ ОЦЕНКЕ ЭФФЕКТИВНОСТИ ЗАТРАТ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ [Электронный ресурс] // Интеллект. Инновации. Инвестиции. — Электрон. дан. — 2015. — № 3. — С. 36-44. — Режим доступа: https://e.lanbook.com/journal/issue/300521. — Загл. с экрана.

7. Степанов-Егиянц, В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации [Электронный ресурс] : монография / В.Г. Степанов-Егиянц. — Электрон. дан. — Москва : СТАТУТ, 2016. — 190 с. — Режим доступа: https://e.lanbook.com/book/92503. — Загл. с экрана

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– 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.

16. 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	Лекции, практические занятия, лабораторные занятия, групповые и индивидуальные консультации, текущий контроль, промежуточна	**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	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

(гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2.** ***учебная аудитория для проведения лабораторных работ:*** компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **2.** ***учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **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	я аттестация	встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт APAPT MA1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт APAPT MA1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с	бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License..

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), 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). **7.*помещение для хранения и профилактического обслуживания учебного оборудования:***аудитория № 523(гуманитарный корпус).		пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610** Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Аудитория 402 читальный зал библиотеки** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.	

Приложение 1

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

Содержание рабочей программы дисциплины
Информационная безопасность предприятия
на 8 семестр - ОФО

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	49,2
лекций	12
практических / семинарских	18
лабораторных	18
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	1,2
Учебных часов на самостоятельную работу	60
Учебных часов на подготовку к экзамену	34,8

Форма контроля
Экзамен 8 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	**Основные направления, принципы и условия организационной защиты информации на предприятии** Основные принципы организационной защиты информации Основные подходы и требования к организации системы защиты информации Основные методы, силы и средства, используемые для организации защиты информации		4	4	4	15	1-4	Изучить правовые аспекты организационной защиты информации на предприятии	Лабораторная работа, Письменная контрольная работа
2	**Организация службы безопасности предприятия** Функции, задачи и особенности службы		2	4	4	15	1-4	Изучить современные модели организации доступа к	Лабораторная работа, Письменная контрольная работа

	безопасности объекта. Принципы организации службы безопасности объекта. Типовая структура службы безопасности Права, обязанности и ответственность сотрудников службы безопасности Способы и формы взаимодействия службы безопасности объекта с правоохранительными органами.							информации	
3	**Организационная защита информации на предприятии** Подбор сотрудников и работа с кадрами Организация внутриобъектового режима Работа с посетителями Организация охраны объектов Организация пропускного режима		2	4	6	15	1-7	Изучить современные модели организации доступа к информации	Лабораторная работа, Письменная контрольная работа
4	**Организация аналитической работы в области защиты информации на предприятии**		4	6	4	15	1-7	Изучить классификации методов анализа информации	Лабораторная работа, Письменная контрольная работа

	Основные направления аналитической работы Функции аналитического подразделения Основные этапы аналитической работы Содержание и основные виды аналитических отчетов								
	итого		12	18	18	60			

Приложение 2

Рейтинг – план дисциплины

Информационная безопасность предприятия

Направление подготовки 10.03.01 Информационная безопасность

Курс 4, семестр 8

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Основные направления, принципы и условия организационной защиты информации на предприятии				
Текущий контроль				
1. Аудиторная работа	6	1	1	6
2. Лабораторная работа №1	14	1	0	14
Рубежный контроль				
1. Письменная контрольная работа №1	15	1	0	15
Всего				35
Модуль 2. Организация аналитической работы в области защиты информации на предприятии				
Текущий контроль				
1. Аудиторная работа	6	1	1	6
2. Лабораторная работа №2	14	1	0	14
Рубежный контроль				
1. Письменная контрольная работа №2	15	1	0	15
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