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

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

Согласовано:
Председатель УМК института
_____ / Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Теория информационной безопасности и методология защиты информации
Б1.Б.17 базовая
Программа специалитета

Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация
Технологии защиты информации в правоохранительной сфере

Квалификация
Специалист по защите информации

Разработчик (составитель)

Доцент, канд.физ.-мат.наук, доцент _____ / Шагапов И.А.

Для приема: 2020 г.

Уфа 2020 г.

Составитель: И.А.Шагапов

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

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

Заведующий кафедрой ___________________/ _____________Ф.И.О/

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

Заведующий кафедрой ___________________/ _____________Ф.И.О/

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

Заведующий кафедрой ___________________/ _____________Ф.И.О/

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

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Список документов и материалов

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

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

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	Знать способы проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	ОПК-2. Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации.	
	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности	ПК-1. Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	
	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	ПК-3. Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации.	
	Знать тенденции в области развития информационных систем и динамику проблем информационной безопасности, общеметодологические принципы теории информационной безопасности и состояние законодательной базы и стандарты в области информационной безопасности	ПК-18. Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации.	
Умения	Уметь проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	ОПК-2. Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты	

		информации.	
	Уметь реализовывать на практике принципы политики безопасности, обосновывать организационно-технические мероприятия по защите информации	ПК-1. Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	
	Уметь реализовывать на практике принципы политики безопасности, использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	ПК-3. Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации.	
	Уметь использовать базовые возможности информационных систем для решения задач фирмы и внедрять компоненты АИС предприятия, обеспечивающие информационную безопасность и достижение стратегических целей и организовать поддержку обеспечения выполнения этой организацией своих функций на основе безопасных АИС	ПК-18. Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации.	
Владения (навыки / опыт деятель-ности)	Владеть навыками проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	ОПК-2. Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации.	
	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления, навыками выявления и устранения угроз информационной безопасности	ПК-1. Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и	

		вероятных угроз.	
	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	ПК-3. Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации.	
	Владеть навыками выявления и устранения угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности; обосновывать организационно-технические мероприятия по защите информации	ПК-18. Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации.	

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Теория информационной безопасности и методология защиты информации» относится к обязательным дисциплинам базовой части.

Дисциплина изучается на 2,3 курсах в 4,5 семестрах.

Целью учебной дисциплины «Теория информационной безопасности и методология защиты информации» является раскрытие сущности и значения понятий информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация составляющих информационной безопасности и защиты информации, установление логической взаимосвязи входящих в них компонентов.

Изучение дисциплины базируется на знаниях, умениях и навыках, сформированных в результате освоения студентами предшествующих дисциплин образовательной программы.

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-2. Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов экзамена и защиты курсового проекта			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать способы проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и	Фрагментарные представления о способах проведения мероприятий по охране труда и технике	Неполные представления о способах проведения мероприятий по охране труда и технике безопасности	Сформированные, но содержащие отдельные неточности о способах проведения мероприятий по охране	Сформированные представления о способах проведения мероприятий по охране труда и технике

	технического обслуживания средств обработки и защиты информации	безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации ном языке.	в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации
Второй этап (уровень)	Уметь проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	Фрагментарное умение проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	В целом успешное, но не систематическое умение проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	В целом успешное, но содержащее отдельные пробелы в умении проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	Сформированное умение проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации
Третий этап (уровень)	Владеть навыками проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	Фрагментарное владение навыками проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	В целом успешное, но не систематическое владение навыками проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	В целом успешное, но содержащее отдельные пробелы владения навыками проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	Успешное и систематическое владение навыками проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации

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

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 основные политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности	Знает основные 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, обосновывать организационно-технические мероприятия по защите информации	Не показывает сформированные умения реализовывать на практике принципы политики безопасности, обосновывать организационно-технические мероприятия по защите информации	Умеет использовать некоторые приемы реализовывать на практике принципы политики безопасности, обосновывать организационно-технические мероприятия по защите информации	Уверенно использует большинство приемов реализовывать на практике принципы политики безопасности, обосновывать организационно-технические мероприятия по защите информации	Уверенно умеет реализовывать на практике принципы политики безопасности, обосновывать организационно-технические мероприятия по защите информации
Третий этап (уровень)	Владеть навыками анализа, обработки и интерпретации результатов решения	Не владеет основными навыками анализа, обработки и интерпретации результатов	Владеет основными навыками анализа, обработки и интерпретации результатов	Владеет основными навыками анализа, обработки и интерпретации результатов	Уверенно владеет навыками анализа, обработки и интерпретации результатов

	прикладных задач управления, навыками выявления и устранения угроз информационной безопасности	решения прикладных задач управления, навыками выявления и устранения угроз информационной безопасности	решения прикладных задач управления, навыками выявления и устранения угроз информационной безопасности, но допускает ошибки	решения прикладных задач управления, навыками выявления и устранения угроз информационной безопасности	решения прикладных задач управления, навыками выявления и устранения угроз информационной безопасности

ПК-3. Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации.

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, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	Фрагментарно знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	В целом знает основные политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур.	Знает основные политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	Уверенно знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур
Второй этап (уровень)	Уметь реализовывать на практике принципы политики безопасности,	Не показывает сформированные умения реализовывать на практике принципы	Умеет использовать некоторые методы реализовывать на практике	Уверенно использует большинство методов реализовывать на практике	Уверенно умеет реализовывать на практике принципы политики

	использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	политики безопасности, использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	принципы политики безопасности, использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	принципы политики безопасности, использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	безопасности, использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности
Третий этап (уровень)	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	Не владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	Владеет основными навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации, но допускает значительные	Владеет основными навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	Уверенно владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации

			ошибки.		

ПК-18. Способность разрабатывать предложения по совершенствованию системы управления безопасностью 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 тенденции в области развития информационных систем и динамику проблем информационной безопасности, общеметодологические принципы теории информационной безопасности и состояние законодательной базы и стандарты в области информационной безопасности	Фрагментарно знает тенденции в области развития информационных систем и динамику проблем информационной безопасности, общеметодологические принципы теории информационной безопасности и состояние законодательной базы и стандарты в области информационной безопасности	В целом знает тенденции в области развития информационных систем и динамику проблем информационной безопасности, общеметодологические принципы теории информационной безопасности и состояние законодательной базы и стандарты в области информационной безопасности	Знает основные тенденции в области развития информационных систем и динамику проблем информационной безопасности, общеметодологические принципы теории информационной безопасности и состояние законодательной базы и стандарты в области информационной безопасности	Уверенно знает тенденции в области развития информационных систем и динамику проблем информационной безопасности, общеметодологические принципы теории информационной безопасности и состояние законодательной базы и стандарты в области информационной безопасности
Второй этап (уровень)	Уметь использовать базовые возможности информационных систем для решения задач фирмы и внедрять компоненты АИС предприятия, обеспечивающ	Не показывает сформированные умения использовать базовые возможности информационных систем для решения задач фирмы и внедрять компоненты АИС	Умеет использовать базовые возможности информационных систем для решения задач фирмы и внедрять компоненты АИС предприятия, обеспечивающ	Уверенно использует базовые возможности информационных систем для решения задач фирмы и внедрять компоненты АИС предприятия, обеспечивающ	Уверенно умеет использовать базовые возможности информационных систем для решения задач фирмы и внедрять компоненты АИС предприятия,

	ие информационную безопасность и достижение стратегических целей и организовать поддержку обеспечения выполнения этой организацией своих функций на основе безопасных АИС	предприятия, обеспечивающие информационную безопасность и достижение стратегических целей и организовать поддержку обеспечения выполнения этой организацией своих функций на основе безопасных АИС	ие информационную безопасность и достижение стратегических целей и организовать поддержку обеспечения выполнения этой организацией своих функций на основе безопасных АИС	ие информационную безопасность и достижение стратегических целей и организовать поддержку обеспечения выполнения этой организацией своих функций на основе безопасных АИС	обеспечивающие информационную безопасность и достижение стратегических целей и организовать поддержку обеспечения выполнения этой организацией своих функций на основе безопасных АИС
Третий этап (уровень)	Владеть навыками выявления и устранения угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности; обосновывать организационно-технические мероприятия по защите информации	Не владеет основными навыками выявления и устранения угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности; обосновывать организационно-технические мероприятия по защите информации	Владеет основными навыками выявления и устранения угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности; обосновывать организационно-технические мероприятия по защите информации, но допускает значительные ошибки.	Владеет навыками выявления и устранения угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности; обосновывать организационно-технические мероприятия по защите информации	Уверенно владеет навыками выявления и устранения угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности; обосновывать организационно-технические мероприятия по защите информации

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 способы проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	ОПК-2. Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации.	Практическая 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-1. Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	Практическая задание, Письменная контрольная работа, Лабораторная работа
	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	ПК-3. Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации.	Практическая задание, Письменная контрольная работа, Лабораторная работа
	Знать тенденции в области развития информационных систем и динамику проблем информационной безопасности, общеметодологические принципы теории информационной безопасности и состояние законодательной базы и стандарты в области информационной безопасности	ПК-18. Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации.	Практическая задание, Письменная контрольная работа, Лабораторная работа

2 этап Умения	Уметь проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	ОПК-2. Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации.	Практическая задание, Письменная контрольная работа, Лабораторная работа
	Уметь реализовывать на практике принципы политики безопасности, обосновывать организационно-технические мероприятия по защите информации	ПК-1. Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	Практическая задание, Письменная контрольная работа, Лабораторная работа
	Уметь реализовывать на практике принципы политики безопасности, использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	ПК-3. Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации.	Практическая задание, Письменная контрольная работа, Лабораторная работа
	Уметь использовать базовые возможности информационных систем для решения задач фирмы и внедрять компоненты АИС предприятия, обеспечивающие информационную безопасность и достижение стратегических целей и организовать поддержку обеспечения выполнения этой организацией своих функций на основе безопасных АИС	ПК-18. Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации.	Практическая задание, Письменная контрольная работа, Лабораторная работа
3 этап Владения навыками	Владеть навыками проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	ОПК-2. Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации.	Практическая задание, Письменная контрольная работа, Лабораторная работа
	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления,	ПК-1. Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную	Практическая задание, Письменная контрольная

	навыками выявления и устранения угроз информационной безопасности	защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	работа, Лабораторная работа
	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	ПК-3. Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации.	Практическая задание, Письменная контрольная работа, Лабораторная работа
	Владеть навыками выявления и устранения угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности; обосновывать организационно-технические мероприятия по защите информации	ПК-18. Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации.	Практическая задание, Письменная контрольная работа, Лабораторная работа

Экзамен

Структура экзаменационного билета
Экзаменационный билет состоит из двух вопросов

Типовые экзаменационные материалы
Вопросы к экзамену 4 семестр

1. Информационная безопасность и её составляющие
2. Безопасность в информационном обществе
3. Информация в современном мире и её свойства
4. Понятие безопасности
5. Информационная безопасность: понятие и составляющие
6. Место информационной безопасности в системе национальной безопасности России
7. Информационная война как угроза национальной безопасности
8. Место информационной безопасности в системе национальной безопасности
9. Значение информационной безопасности для субъектов информационных отношений
10. Концептуальная модель и основные понятия

11. Объекты и угрозы информационной безопасности России
12. Политика обеспечения информационной безопасности Российской Федерации
13. Система обеспечения информационной безопасности Российской Федерации
14. Концептуальная модель и основные понятия
15. Объекты и угрозы информационной безопасности организации
16. Политика обеспечения информационной безопасности организации
17. Система обеспечения информационной безопасности организации
18. Модель безопасности информационных технологий организации
19. Методология защиты информации.
20. Понятие и сущность защиты информации
21. Общий контекст защиты информации
22. Понятие и сущность защиты информации как вида деятельности
23. Цели и задачи защиты информации
24. Концептуальная модель защиты информации
25. Основные положения теории защиты информации
26. Методологический базис теории защиты информации
27. Модели систем и процессов защиты информации
28. Состав и основные свойства защищаемой информации
29. Основные свойства информации, обуславливающие необходимость её защиты
30. Понятие и состав защищаемой информации.
31. Принципы отнесения информации к защищаемой
32. Носители защищаемой информации
33. Классификация информации ограниченного доступа по видам тайны и степеням конфиденциальности
34. Показатели разделения информации ограниченного доступа на виды тайны
35. Государственная тайна
36. Коммерческая тайна
37. Персональные данные
38. Служебная тайна
39. Профессиональная тайна

Вопросы к экзамену 5 семестр

1. Понятие, классификация и оценка угроз безопасности информации
2. Понятие угрозы и её взаимосвязь с уязвимостью и рисками
3. Общая классификация угроз безопасности информации
4. Цели и задачи оценки угроз безопасности информации
5. Источники и способы реализации угроз безопасности информации. Уязвимости систем обработки информации
6. Источники угроз безопасности информации
7. Виды угроз безопасности информации и способы их реализации со стороны субъективных источников
8. Уязвимости систем обработки информации
9. Каналы утечки информации и методы несанкционированного доступа к информации ограниченного доступа
10. Каналы утечки информации ограниченного доступа
11. Методы несанкционированного доступа к конфиденциальной информации
12. Неформальная модель нарушителя безопасности автоматизированной системы

13. Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации
14. Структура разведывательных служб частных объединений
15. Направления и виды разведывательной деятельности
16. Способы несанкционированного доступа к конфиденциальной информации агентурной разведки
17. Компьютерная разведка информации
18. Назначение и структура систем защиты информации
19. Понятие и общая структура системы защиты информации
20. Типизация, стандартизация, классификация систем защиты.
21. Объекты защиты информации
22. Понятие и общая классификация объектов защиты информации
23. Средства и системы обработки информации как объекты защиты информации
24. Средства обеспечения объекта информатизации
25. Помещения, в которых установлены средства обработки, и помещения для конфиденциальных переговоров как объекты защиты информации
26. Классификация видов, способов, методов и средств защиты информации
27. Виды защиты информации и сферы их действия
28. Общие способы защиты информации
29. Общая классификация средств защиты информации
30. Характеристика способов и средств по видам защиты

Пример экзаменационного билета

МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ
Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере
Теория информационной безопасности и методология защиты информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. *Понятие, классификация и оценка угроз безопасности информации*
2. *Уязвимости систем обработки информации*

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
Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере
Теория информационной безопасности и методология защиты информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. *Помещения, в которых установлены средства обработки, и помещения для конфиденциальных переговоров как объекты защиты информации*
2. *Направления и виды разведывательной деятельности*

Зав. кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

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.

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.

Примерная тематика курсовых проектов

1. Особенности защиты коммерческой тайны предприятия
2. Особенности защиты персональных данных
3. Лицензирование в области информационной безопасности
4. Сертификация в области информационной безопасности
5. Модели угроз информационной безопасности
6. Модели нарушителя информационной безопасности
7. Особенности построения комплексной системы защиты информации
8. Информационная война в современных условиях
9. Физическая защита информации
10. Особенности защиты информации в чрезвычайных ситуациях
11. Экономическая эффективность защиты информации
12. Аттестация объектов информатизации по требованиям безопасности

13. Особенности аудита информационной безопасности
14. Особенности защиты информации в сфере туризма
15. Особенности обеспечения безопасности Интернета вещей
16. Организационно-правовые вопросы применения полиграфа
17. Мониторинг и анализ данных социальных сетей
18. Организационно-правовые вопросы инженерно-технической защиты информации
19. Управление рисками информационной безопасности
20. Особенности защиты информации при проведении конфиденциальных переговоров
21. Уязвимости и угрозы информационной безопасности в области организационной защиты информации
22. Анализ уязвимостей в области технической защиты информации
23. Особенности защиты государственной тайны
24. Управление персоналом, допущенным к конфиденциальной информации
25. Направления и виды разведывательной деятельности
26. Методы выявления нарушителей, тактики их действий и состава интересующей их информации
27. Управление системой защиты информации в условиях чрезвычайных ситуаций
28. Подходы к оценке ущерба от нарушений ИБ

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 информационной безопасности

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	3
Выполнены пункты 1-3	5
Максимальный балл	5

Модуль 2.
Теоретические основы информационной безопасности организации
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	3
Выполнены пункты 1-3	5
Максимальный балл	5

Модуль 3.
Методология защиты 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	6
Выполнены пункты 1-3	10
Максимальный балл	10

Модуль 4.

Назначение и структура систем защиты 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	6
Выполнены пункты 1-4	10
Максимальный балл	10

Комплект практических заданий

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

Модуль 1
Основы информационной безопасности
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	3
Выполнены пункты 1-3	5
Максимальный балл	5

Модуль 2.
Теоретические основы информационной безопасности организации
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	3
Выполнены пункты 1-3	5
Максимальный балл	5

Модуль 3.
Методология защиты 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	6
Выполнены пункты 1-3	10
Максимальный балл	10

Методические указания

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

Модуль 3.
Методология защиты 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	6
Выполнены пункты 1-5	10
Максимальный балл	10

Модуль 4.
Назначение и структура систем защиты информации

Типовое практическое задание 5
Классификация тайн

1.Государственная тайна. Понятие государственнойб тайны.
Отнесение сведений к государственной тайне: понятие, принципы отнесения, степени секретности.
2.Коммерческая тайна. Понятие коммерческой тайны и информации составляющей коммерческую тайну. Отнесение сведений к коммерческой тайне.
3.Персональные данные. Понятия персональных данных. Охрана конфиденциальности персональных данных.
4. Служебная тайна. Понятие служебной тайны. Объекты служебной тайны.
5.Профессиональная тайна. Понятие профессиональной тайны. Объекты профессиональной тайны.

Методические рекомендации по подготовке к занятиям

При подготовке особое внимание обратить на:
1) классификацию информации по видам тайны;
2) степени конфиденциальности различных видов тайны;
3) порядок отнесения сведений к государственной тайне и информации, составляющей коммерческую тайну;
4) объекты служебной и профессиональной тайны.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	6
Выполнены пункты 1-5	10
Максимальный балл	10

Модуль 4.
Назначение и структура систем защиты информации
Типовое практическое задание 6
Методология защиты информации

1.Основные положения и особенности теории защиты информации.
Понятие, задачи и составные части теории защиты информации. Особенности теории защиты информации.
2. Методологический базис теории защиты информации.
Методы лингвистических переменных (нестрогой математики).
Методы неформального оценивания. Неформальные методы поиска оптимальных решений.
3. Модели систем и процессов защиты информации.
Классификация моделей. Общая модель процесса защиты информации. Частные модели защиты.

Методические рекомендации по подготовке к занятиям

При подготовке особое внимание обратить на:
1) особенности теории защиты;
2) методы лингвистических переменных (нестрогой математики);
3) общую модель процесса защиты информации.
4) вопросы для дискуссии.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	6

Выполнены пункты 1-5	10
Максимальный балл	10

Комплект лабораторных работ

Для закрепления на практике умений предусмотрены несколько лабораторных работ.

Модуль 1
Основы информационной безопасности
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	4
Выполнены пункты 1-4	10
Максимальный балл	10

Модуль 1.
Основы информационной безопасности
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	4
Выполнены пункты 1-5	10
Максимальный балл	10

Модуль 2.
Теоретические основы информационной безопасности организации
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 2.
Теоретические основы информационной безопасности организации
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

4.3. Рейтинг-план дисциплины

Рейтинг-план дисциплины представлен в приложении 2.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. 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. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. - Москва : Горячая линия - Телеком, 2011. - 558 с. : ил. - ISBN 5-93517-292-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253056
3. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Национальный исследовательский университет – Высшая школа экономики. - Москва : Издательский дом Высшей школы экономики, 2015. - 574 с. : ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285

Дополнительная литература

1. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - Москва : Горячая линия-Телеком, 2015. - 585 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0424-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457143
2. Щербаков, А. Современная компьютерная безопасность. Теоретические основы.

Практические аспекты : учебное пособие / А. Щербаков. - Москва : Книжный мир, 2009. - 352 с. - (Высшая школа). - ISBN 978-5-8041-0378-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=89798

3. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331

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. Лицензии бессрочные.

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

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения Реквизиты подтверждающего документа
1	2	3
1. Учебная аудитория для проведения занятий лекционного типа: Аудитория № 405. 450076, Республика Башкортостан, г. Уфа, ул. Карла Маркса, д. 3, корп. 4 (4 этаж № 7).	Аудитория № 405. Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интерактивная система со встроенным короткофокусным проектором 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., Двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2nd Generation – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт.	Windows 8 Russian Windows Professional 8 Russian Upgrade. Договор №104 от 17.06.2013 г. Лицензии бессрочные. Microsoft Office Standard 2013 Russian. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
2. Учебная аудитория для проведения занятий семинарского типа: Аудитория № 610. 450076, Республика Башкортостан, г. Уфа, ул. Карла Маркса, д. 3, корп. 4 (6 этаж № 52).	Аудитория № 610. Оборудование: учебная мебель, доска, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м	Windows 8 Russian Windows Professional 8 Russian Upgrade. Договор №104 от 17.06.2013 г. Лицензии бессрочные. Microsoft Office Standard 2013 Russian. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
3. Учебная аудитория для проведения групповых и индивидуальных консультаций: Аудитория № 608. 450076, Республика Башкортостан, г. Уфа, ул. Карла Маркса, д. 3, корп. 4 (6 этаж № 49).	Аудитория № 608. Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование	
4. Учебная аудитория для текущего контроля и промежуточной аттестации:	Аудитория № 609. Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование	

Аудитория № 609. 450076, Республика Башкортостан, г. Уфа, ул. Карла Маркса, д. 3, корп. 4 (6 этаж № 50).		
5. Помещения для самостоятельной работы: Аудитория № 402 (читальный зал) 450076, Республика Башкортостан, г. Уфа, ул. Карла Маркса, д. 3, корп. 4. (4 этаж № 5). Аудитория № 613 450076, Республика Башкортостан, г. Уфа, ул. Карла Маркса, д. 3, корп. 4. (6 этаж № 4).	Аудитория № 402 (читальный зал) Оборудование: Учебная мебель, стенд по пожарной безопасности, моноблоки стационарные – 5 шт. с возможностью подключения к сети Интернет и доступа в электронную информационно-образовательную среду, принтер – 1 шт., сканер – 1 шт. Аудитория № 613 Оборудование: учебная мебель, доска, моноблок стационарный – 12 шт. с возможностью подключения к сети Интернет и доступа в электронную информационно-образовательную среду.	
6. Помещение для хранения и профилактического обслуживания учебного оборудования: Аудитория № 523 450076, Республика Башкортостан, г. Уфа, ул. Карла Маркса, д. 3, корп. 4. (5 этаж № 14).	Аудитория № 523 Оборудование: стол, стул, шкаф-стеллаж, мобильное мультимедийное оборудование – проектор, ноутбук, экран переносной	

Приложение 1

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

Содержание рабочей программы дисциплины
Теория информационной безопасности и методология защиты информации
на 4семестр

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	65,2
лекций	16
практических / семинарских	32
лабораторных	16
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	1,2
Учебных часов на самостоятельную работу	26
Учебных часов на подготовку к экзамену	52,8

Форма контроля:
Экзамен 4 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	1		4	5	6	7	8	9	10
1	**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЕЁ СОСТАВЛЯЮЩИЕ** Безопасность в информационном обществе Информация в современном мире и её свойства Основные формы проявления информации Информационная безопасность: понятие и составляющие Информационная безопасность Российской Федерации Информационная безопасность организации Информационная безопасность технической системы		2	4		3	1-3	Изучить историю информационного оружия	Письменная контрольная работа
2	**МЕСТО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ** Информационная война как угроза национальной безопасности Место информационной безопасности в системе		2	4	4	3	1-5	Изучить историю информационных войн	Письменная контрольная работа

	национальной безопасности Значение информационной безопасности для субъектов информационных отношений								
3	**ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ** Концептуальная модель и основные понятия Объекты и угрозы информационной безопасности России Политика обеспечения информационной безопасности России Система обеспечения информационной безопасности России		2	4		3	1-5	Изучить историю информационных войн и оружия	Практическое задание, Письменная контрольная работа, Лабораторная работа
4	**ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ** Концептуальная модель и основные понятия Объекты и угрозы информационной безопасности организации Система обеспечения информационной безопасности организации Модель безопасности системы информационных технологий организации		2	4	4	3	1-5	Изучить современное состояние информационных войн	Практическое задание, Письменная контрольная работа, Лабораторная работа
5	**ПОНЯТИЕ И СУЩНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ**		2	4		3	1-6	Изучить рекомендованную	Практическое задание,

	Общий контекст защиты информации Понятие и сущность защиты информации как вида деятельности Цели и задачи защиты информации Концептуальная модель защиты информации							литературу по дисциплине	Письменная контрольная работа, Лабораторная работа
6	**ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ** Основные положения теории защиты информации Модели систем и процессов защиты информации		2	4	4	3	1-5	Изучить рекомендованную литературу по угрозам ИБ	Практическое задание, Письменная контрольная работа, Лабораторная работа
7	**СОСТАВ И ОСНОВНЫЕ СВОЙСТВА ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ** Основные свойства информации, обуславливающие необходимость её защиты Понятие и состав защищаемой информации. Принципы отнесения информации к защищаемой Носители защищаемой информации Понятие и классификация носителей защищаемой информации		2	4		4	1-4	Для выбранной организации схематично построить модель безопасности ИТ	Практическое задание, Письменная контрольная работа
8	**КЛАССИФИКАЦИЯ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА ПО ВИДАМ ТАЙНЫ И СТЕПЕНЯМ**		2	4	4	4	1-5	Для выбранной организации схематично построить модель безопасности ИТ	Практическое задание, Письменная контрольная работа,

	КОНФИДЕНЦИАЛЬНОСТИ Информация ограниченного доступа Показатели разделения ИОД на тайны Государственная тайна Коммерческая тайна Персональные данные Служебная тайна Профессиональная тайна							органгизации	Лабораторная работа
	всего		16	32	16	26			

Содержание рабочей программы дисциплины
Теория информационной безопасности и методология защиты информации
на 5 семестр

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	57,2
лекций	18
практических / семинарских	36
лабораторных	-
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	3,2
Учебных часов на самостоятельную работу	25
Учебных часов на подготовку к экзамену	25,8

Форма контроля:
Экзамен 5 семестр
В том числе: курсовой проект 5 семестр, контактных часов – 2.

№	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	1		4	5	6	7	8	9	10
1	**ПОНЯТИЕ, КЛАССИФИКАЦИЯ И ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ** Понятие угрозы безопасности информации Взаимосвязь угроз безопасности информации, уязвимости и риска Идентификация уязвимостей и угроз Структурно - логическая схема угрозы безопасности информации Общая классификация угроз безопасности информации Цели и задачи оценки угроз безопасности		2	2		1	1-3	Какая информация в организации подлежит защите?	Практическое задание, Письменная контрольная работа

	информации								
2	**ИСТОЧНИКИ И СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, УЯЗВИМОСТИ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ** Источники угроз безопасности информации Классификация источников угроз безопасности информации Виды угроз безопасности информации со стороны субъективных внешних источников и способы их реализации Классы уязвимостей систем обработки информации и их характеристика		2	4		3	1-4	Для чего нужны различные классификации?	Практическое задание, Письменная контрольная работа
3	**КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ И МЕТОДЫ НЕСАНКЦИОНИРО**		2	4		3	1-5	Изучить угрозы безопасности организации	Практическое задание, Письменная контрольная

	ВАННОГО ДОСТУПА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ Преднамеренные воздействия на информацию Классификация каналов утечки информации Организационные каналы утечки информации Технические каналы утечки информации Методы НСД и использованием ТКУИ Модели нарушителя								работа
4	**НАПРАВЛЕНИЯ, ВИДЫ И ОСОБЕННОСТИ ДЕЯТЕЛЬНОСТИ РАЗВЕДЫВАТЕЛЬНЫХ СЛУЖБ ПО НЕСАНКЦИОНИРОВАННОМУ ДОСТУПУ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ** Государственные разведывательные		2	4		3	1-5	Изучить литературу по коммерческой тайне организации	Практическое задание, Письменная контрольная работа

	службы зарубежных стран Разведывательные службы иностранных государств Разведывательные организации, входящие в гражданские ведомства США Направления и виды разведывательной деятельности Агентурная разведка								
5	**ОБЪЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ** Объект защиты информации Защищаемая информационная система Защищаемые информационные процессы Защищаемый объект информатизации Классификация объектов информатизации Помещения, в которых установлены средства обработки защищаемой		2	4		3	1-4	Изучить особенности разработки режима коммерческой тайны организации	Практическое задание, Письменная контрольная работа

	информации Помещения, в которых установлены ОТСС Помещения для работы с защищаемой информацией Помещения для конфиденциальных переговоров								
6	**КЛАССИФИКАЦИЯ ВИДОВ, СПОСОБОВ, МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ** Виды защиты информации Правовая защита информации Организационная защита информации Инженерно-техническая защита информации Программно-аппаратная защита информации Криптографическая защита информации		2	6		3	1-6	Изучить особенности классификации защищаемой информации	Практическое задание, Письменная контрольная работа
7	**НАЗНАЧЕНИЕ И СТРУКТУРА СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ**		2	4		3	1-6	Изучить особенности классификации защищаемой	Практическое задание, Письменная контрольная

	Система защиты информации Компоненты системы защиты информации Общеметодологические требования построения систем защиты информации Уровни типизации и стандартизации Классификация СЗИ по уровню обеспечиваемой защиты Классификация СЗИ по активности реагирования							информации	работа
8	**КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ** Определение КСЗИ Подсистема управления Подсистема защиты информации от НСД в АС и ИТКС Подсистема защиты от несанкционированного физического доступа Подсистема		2	4		3	1-4	Построить классификацию защищаемой информации для выбранной организации	Практическое задание, Письменная контрольная работа

	антивирусной защиты Подсистема защиты информации от утечки по техническим каналам Подсистема противодействия техническим разведкам								
9	**УПРАВЛЕНИЕ КОМПЛЕКСНОЙ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ** Классификации ЧС Факторы, влияющие на принятие решения Информационная поддержка принятия решения Подготовка мероприятий на случай возникновения ЧС Мероприятия по подготовке к действиям при ЧС		2	4		3	1-6	Для выбранной организации, выбрать адекватные средства защиты	Практическое задание, Письменная контрольная работа
	всего		18	36		25	1-6		
	Курсовой проект					20	1-6	Курсовой проект по заданной теме	
			18	36		25			

Приложение 2

Рейтинг – план дисциплины

Теория информационной безопасности и методология защиты информации

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Курс 2, семестр 4

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Основы информационной безопасности				
Текущий контроль				
1. Аудиторная работа	5	1	1	5
2. Практическая работа №1	5	1	0	5
3. Лабораторная работа №1	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №1	5	1	0	5
2. Лабораторная работа №2	10	1	0	10
Всего				35
Модуль 2. Теоретические основы информационной безопасности организации				
Текущий контроль				
1. Аудиторная работа	5	1	1	5
2. Практическая работа №2	5	1	0	5
3Лабораторная работа №3	10	1	10	10
Рубежный контроль				
1. Письменная контрольная работа №2	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

Рейтинг – план дисциплины

Теория информационной безопасности и методология защиты информации
Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере
Курс 3, семестр 5

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 3. Методология защиты информации.				
Текущий контроль				
1. Аудиторная работа	5	1	1	5
2. Практическая работа №3	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №3	10	1	0	10
2. Практическая работа №4	10	1	0	10
Всего				35
Модуль 4. Назначение и структура систем защиты информации				
Текущий контроль				
1. Аудиторная работа	5	1	1	5
2. Практическая работа №5	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №4	10	1	0	10
2 Практическая работа №6	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