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

Актуализировано:
на заседании кафедры
протокол №10 от «07»июня2018г.
Зав.кафедрой
_____/А.С.Исмагилова

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

дисциплина **Информационная безопасность в профессиональной деятельности**

вариативная

программа специалитета

Специальность
38.05.01 Экономическая безопасность

Специализация №1
Экономико-правовое обеспечение экономической безопасности

Квалификация
экономист

Разработчик (составитель) к.б.н., доцент	_____/Ф.Т. Байрушин

Для приема: 2014 г.

Уфа 2018 г.

Составитель: Ф.Т. Байрушин

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью, протокол №10 от «7» июня 2018г.

Дополнения и изменения, внесённые в рабочую программу дисциплины, утверждены на заседании кафедры _____,

протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О./

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры _____,

протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О./

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры _____,

протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О./

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы 4

2. Цель и место дисциплины в структуре образовательной программы 5

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся) 5

4. Фонд оценочных средств по дисциплине 5

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 5

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 8

4.3. Рейтинг-план дисциплины (при необходимости) 28

5. Учебно-методическое и информационное обеспечение дисциплины 28

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины 28

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины 29

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине 29

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:

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	1. Знать: понятие информационной безопасности и защиты информации и их значение в деятельности организаций.	ПК - 20: способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	
	2. Знать: общую классификацию угроз информационной безопасности;	ПК-28: способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач	
	3. Знать: понятие информационной безопасности и защиты информации и их значение в деятельности организаций.	ПК-29: способность выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор	
Умения	1. Уметь: определять основные факторы, влияющие на информационную безопасность и защиту информации.	ПК - 20: способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	
	2. Уметь: определять основные факторы, влияющие на информационную безопасность и защиту информации;	ПК-28: способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач	
	3.Уметь: определять основные факторы, влияющие на информационную безопасность и защиту информации.	ПК-29: способность выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор	
Владения (навыки / опыт деятельности)	1. Владеть: способами обеспечения информационной безопасности и защиты информации.	ПК - 20: способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	
	2. Владеть: основными	ПК-28: способность осуществлять сбор,	

	методами, способами и средствами получения, хранения, переработки информации;	анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач	
	3.Владеть:основными методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления документопотоками.	ПК-29: способность выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор	

2. Цель и место дисциплины в структуре образовательной программы

Цель изучения дисциплины: изучение принципов обеспечения информационной безопасности в профессиональной деятельности, видов защищаемой информации, роли информационной безопасности в системе экономической безопасности государства.

Дисциплина «Информационная безопасность в профессиональной деятельности» относится к дисциплинам вариативной части образовательной программы.

Дисциплина изучается на 4-м курсе в 8-ом семестре при очной форме обучения и на 6-ом курсе в 11 семестре при заочной форме обучения.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «Экономическая безопасность», «Стратегические аспекты экономической безопасности», «Информационные системы в экономике», «Экономика организации (предприятия)», «Информатика».

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

Содержание рабочей программы представлено в Приложении А.

4. Фонд оценочных средств по дисциплине

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

ПК - 20:способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения для экзамена			
		2 («Неудовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: понятие информационной безопасности и защиты	Имеет фрагментарные знания понятия информационной безопасности и	В целом знает понятия информационной безопасности и защиты информации	Знает понятия информационной безопасности и защиты информации и	Демонстрирует целостные знания понятия информацион

	информации и их значение в деятельности организаций.	защиты информации и их значение в деятельности организаций	и их значение в деятельности организаций, но допускает значительные ошибки.	их значение в деятельности организаций, допускает незначительные ошибки.	ной безопасности и защиты информации и их значение в деятельности организаций
Второй этап (уровень)	Уметь: определять основные факторы, влияющие на информационную безопасность и защиту информации.	Не способен определять основные факторы, влияющие на информационную безопасность и защиту информации.	В целом умеет определять основные факторы, влияющие на информационную безопасность и защиту информации, но допускает значительные ошибки.	Умеет определять основные факторы, влияющие на информационную безопасность и защиту информации, допускает незначительные ошибки.	Демонстрирует высокий уровень умений определять основные факторы, влияющие на информационную безопасность и защиту информации
Третий этап (уровень)	Владеть: способами обеспечения информационной безопасности и защиты информации.	Не владеет способами обеспечения информационной безопасности и защиты информации.	В целом владеет способами обеспечения информационной безопасности и защиты информации, но испытывает значительные затруднения.	Владеет навыками способами обеспечения информационной безопасности и защиты информации, испытывает незначительные затруднения.	Демонстрирует высокий уровень владения способами обеспечения информационной безопасности и защиты информации.

ПК-28: способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения для экзамена			
		2 («Неудовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: общую классификацию угроз информационной безопасности	Имеет фрагментарные знания об общей классификации угроз информационной безопасности.	В целом общую классификацию угроз информационной безопасности, но допускает значительные ошибки.	Знает общую классификацию угроз информационной безопасности, допускает незначительные ошибки.	Демонстрирует целостные знания общей классификации угроз информационной безопасности.
Второй этап (уровень)	Уметь:определять основные факторы, влияющие на информаци	Не способен определять основные факторы, влияющие на информационную безопасность и защиту информации	В целом умеет определять основные факторы, влияющие на информационную безопасность и защиту информации,	Умеет определять основные факторы, влияющие на информационную безопасность	Демонстрирует высокий уровень умений определять основные факторы,

	онную безопасность и защиту информации		но допускает значительные ошибки.	и защиту информации, допускает незначительные ошибки.	влияющие на информационную безопасность и защиту информации
Третий этап (уровень)	Владеть: основными методами, способами и средствами получения, хранения, переработки информации	Не владеет основными методами, способами и средствами получения, хранения, переработки информации.	В целом владеет основными методами, способами и средствами получения, хранения, переработки информации, но испытывает значительные затруднения.	Владеет основными методами, способами и средствами получения, хранения, переработки информации, испытывает незначительные затруднения.	Демонстрирует высокий уровень владения основными методами, способами и средствами получения, хранения, переработки информации.

ПК-29: способность выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения для экзамена			
		2 («Неудовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: понятие информационной безопасности и защиты информации и их значение в деятельности организаций	Имеет фрагментарные знания о понятии информационной безопасности и защиты информации и их значение в деятельности организаций	В целом знает понятие информационной безопасности и защиты информации и их значение в деятельности организаций, но допускает значительные ошибки.	Знает понятие информационной безопасности и защиты информации и их значение в деятельности организаций, допускает незначительные ошибки.	Демонстрирует целостные знания понятий информационной безопасности и защиты информации и их значение в деятельности организаций
Второй этап (уровень)	Уметь: определять основные факторы, влияющие на информационную безопасность и защиту информации.	Не способен определять основные факторы, влияющие на информационную безопасность и защиту информации	В целом умеет определять основные факторы, влияющие на информационную безопасность и защиту информации, но допускает значительные ошибки.	Умеет определять основные факторы, влияющие на информационную безопасность и защиту информации, допускает незначительные ошибки.	Демонстрирует высокий уровень умений определять основные факторы, влияющие на информационную безопасность и защиту информации
Третий этап	Владеть: основными	Не владеет основными	В целом владеет основными	Владеет навыками	Демонстрирует высокий

(уровень)	методами, способами и средствами получения, хранения, переработки и информации, иметь навыки работы с компьютером как средством управления документопотоками.	методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления документопотоками	методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления документопотоками, но испытывает значительные затруднения.	основными методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления документопотоками, испытывает незначительные затруднения.	уровень владения основными методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления документопотоками

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

Шкала оценивания для экзамена для студентов ОФО:
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.

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

Для очной формы обучения

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
Знать	1. Знать: понятие информационной безопасности и защиты информации и их значение в деятельности организаций.	ПК - 20: способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, участие в круглом столе, творческое задание (доклад), контрольная работа, деловая игра, лабораторная работа

	2. Знать: общую классификацию угроз информационной безопасности;	ПК-28: способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, участие в круглом столе, творческое задание (доклад), контрольная работа, деловая игра, лабораторная работа
	3. Знать: понятие информационной безопасности и защиты информации и их значение в деятельности организаций.	ПК-29: способность выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, участие в круглом столе, творческое задание (доклад), контрольная работа, деловая игра, лабораторная работа
2-й этап Уметь	1. Уметь: определять основные факторы, влияющие на информационную безопасность и защиту информации.	ПК - 20: способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, участие в круглом столе, творческое задание (доклад), контрольная работа, деловая игра, лабораторная работа
	2. Уметь: определять основные факторы, влияющие на информационную безопасность и защиту информации;	ПК-28: способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, участие в круглом столе, творческое задание (доклад), контрольная работа, деловая игра, лабораторная работа
	3.Уметь:определять основные факторы, влияющие на	ПК-29: способность выбирать инструментальные средства для обработки	Аудиторная работа на лекционных занятиях, проводимых в

	информационную безопасность и защиту информации.	финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор	интерактивной форме, тестирование, участие в круглом столе, творческое задание (доклад), контрольная работа, деловая игра, лабораторная работа
3-й этап Владеть	1. Владеть: способами обеспечения информационной безопасности и защиты информации.	ПК - 20: способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, участие в круглом столе, творческое задание (доклад), контрольная работа, деловая игра, лабораторная работа
	2. Владеть: основными методами, способами и средствами получения, хранения, переработки информации;	ПК-28: способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, участие в круглом столе, творческое задание (доклад), контрольная работа, деловая игра, лабораторная работа
	3.Владеть:основными методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления документопотоками.	ПК-29: способность выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, участие в круглом столе, творческое задание (доклад), контрольная работа, деловая игра, лабораторная работа

Для заочной формы обучения

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
Знать	1. Знать: понятие информационной	ПК - 20: способность соблюдать в	Тестирование, участие в круглом столе,

	безопасности и защиты информации и их значение в деятельности организаций.	профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	контрольная работа, лабораторная работа
	2. Знать: общую классификацию угроз информационной безопасности;	ПК-28: способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач	Тестирование, участие в круглом столе, контрольная работа, лабораторная работа
	3. Знать: понятие информационной безопасности и защиты информации и их значение в деятельности организаций.	ПК-29: способность выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор	Тестирование, участие в круглом столе, контрольная работа, лабораторная работа
2-й этап Уметь	1. Уметь: определять основные факторы, влияющие на информационную безопасность и защиту информации.	ПК - 20: способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Тестирование, участие в круглом столе, контрольная работа, лабораторная работа
	2. Уметь: определять основные факторы, влияющие на информационную безопасность и защиту информации;	ПК-28: способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач	Тестирование, участие в круглом столе, контрольная работа, лабораторная работа
	3.Уметь:определять основные факторы, влияющие на информационную безопасность и защиту информации.	ПК-29: способность выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор	Тестирование, участие в круглом столе, контрольная работа, лабораторная работа
3-й этап Владеть	1. Владеть: способами обеспечения информационной безопасности и защиты информации.	ПК - 20: способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми	Тестирование, участие в круглом столе, контрольная работа, лабораторная работа

		актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	
	2. Владеть: основными методами, способами и средствами получения, хранения, переработки информации;	ПК-28: способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач	Тестирование, участие в круглом столе, контрольная работа, лабораторная работа
	3.Владеть:основными методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления документопотоками.	ПК-29: способность выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор	Тестирование, участие в круглом столе, контрольная работа, лабораторная работа

Экзамен

Типовые материалы к экзамену

1.Научные и законодательные определения информации. Соотношение понятий «информация», «документированная информация», «информационные ресурсы», «документ».
2. Сущность и понятие информационной безопасности. Связь информационной безопасности с информатизацией общества.
3. Понятие и назначение доктрины информационной безопасности. Основные положения доктрины информационной безопасности Российской Федерации и их реализация.
4. Сущность и понятие защиты информации. Уязвимость информации. Цели защиты информации.
5. Законодательная база защиты документированной информации в РФ.
6. Подзаконные нормативно-правовые акты в сфере защиты информации.
7. Понятие и виды конфиденциальной информации в современном российском законодательстве.
8. Государственная тайна, ее нормативное регулирование.
9. Правовой режим персональных данных. Общая характеристика Федерального закона «О персональных данных»
10. Понятие коммерческой тайны. Общая характеристика Федерального закона «О коммерческой тайне».
11.Особенности современных информационных систем, существенные с точки зрения безопасности
12.Защита от НСД средствами СУБД
13. Перспективы развития средств защиты от НСД
14.Двусторонняя идентификация и аутентификация
15.Парольная аутентификация
16.Основные требования к криптографическому закрытию информации
17.Протокол для асимметричных криптосистем с использованием сертификатов открытых ключей.
18.Модели безопасности, применяемые при построении защиты в СУБД.
19.Транзакция и восстановление.
20.Стандарты безопасности и их роль.
21.Концепция защиты от НСД к информации.
22. Технологии тиражирования и синхронизации данных Кластерная организация серверов баз данных.
23. Программно-аппаратные средства криптографической защиты информации.
24. Требования, предъявляемые к удостоверяющему центру.

25. Архитектура подсистемы безопасности ОС Windows.
26. Создание защищенной операционной системы.
27. Способы фиксации фактов доступа к файлам. Журналы доступа.
28. Способы защиты информации на съемных дисках.
29.Дискретное, мандатное и ролевое разграничение доступа к объектам КС.
30. Способы идентификации и аутентификации субъектов КС.
преобразований
31.Привязка" к компьютеру (физические дефекты винчестера, дата создания BIOS, серийный номер диска, тип компьютера и др.)
32. Противодействие анализу двоичного кода
33.Реализация механизмов безопасности на аппаратном уровне.
34.Принцип работы систем обнаружения вторжений.
35.Анализ защищенности системы при помощи сканера безопасности.
36.Взаимная проверка подлинности пользователей.
37.Протокол для асимметричных криптосистем с использованием сертификатов открытых ключей.
38 Идентификация и аутентификация с помощью биометрических данных
39.Сравнительная характеристика подсистем защиты распространенных сетевых ОС
40. Понятие и классификация межсетевых экранов.

Типовые задачи к экзамену

1.Предложите схему удаленного администрирования сети филиала. Выбор схемы и соответствующего ПО обоснуйте.
2. Опишите каким образом осуществлено разграничение доступа к информационным ресурсам на вашей ПЭВМ, в случае отсутствия его обоснуйте.
3. Опишите антивирусные программы, которые вы использовали и используете в данный момент. Ваш выбор обоснуйте.

Экзаменационные билеты

Структура экзаменационного билета

Экзаменационный билет состоит из двух вопросов, отражающих материал первого и второго модуля и одной задачи.

Федеральное государственное бюджетное образовательное учреждение высшего образования
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Институт истории и государственного управления

Специальность 38.05.01
Экономическая безопасность
Дисциплина Информационная безопасность в правоохранительной деятельности

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1.Научные и законодательные определения информации. Соотношение понятий «информация», «документированная информация», «информационные ресурсы», «документ».
2. Понятие и классификация межсетевых экранов.
3.Определите в каких формах представлена информация на вашей домашней ЭВМ. Опишите, как обеспечивается информационная безопасность вашей ПЭВМ и отвечает ли современным требованиям развития систем безопасности.

Зав. кафедрой УИБ А.С. Исмагилова

Критерии оценивания результатов экзамена для ОФО:

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 при выполнении практических заданий. 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. При выполнении практической части работы допущены несущественные ошибки;

- 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. Студент не решил задачу или при решении допущены грубые ошибки;

- 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 при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос

Устанавливается следующая градация перевода оценки из многобалльной в четырехбалльную:

Экзамены:

- 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 результатов экзамена для ЗФО:

Оценка «отлично» выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок;

Оценка «хорошо» выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки;

Оценка «удовлетворительно» 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. Студент не решил задачу или при решении допущены грубые ошибки;

Оценка «неудовлетворительно» выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.

Типовые задания для контрольной работы ОФО

Цель проведения контрольной работы – оценка уровня владения базовой профессиональной терминологией в сфере информационной безопасности. Контрольная работа проводится в письменной форме.

Примеры заданий

Модуль 1.

№	Термин	Определение
1.	Абонентское шифрование	защита информации, передаваемой средствами телекоммуникаций криптографическими методами, непосредственно между отправителем и получателем.
2.	Автоматизированная информационная система, АИС	совокупность программных и аппаратных средств, предназначенных для создания, передачи, обработки, распространения, хранения и/или управления данными и информацией и производства вычислений.
3.	Секретная информация	информация, которая представляет собой государственную или служебную тайны и охраняется государством. В зависимости от величины политического или экономического ущерба, который может быть нанесен интересам государства в случае разглашения секретной информации она может иметь гриф особой важности, совершенно секретно или секретно.
4.	Информационные ресурсы	отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). Информационные ресурсы могут быть государственными и негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений. Отношения по поводу права собственности на информационные ресурсы регулируются соответствующим гражданским законодательством.

Модуль 2

Письменная контрольная работа (знание терминов)

№	Термин	Определение
1.	Ключ (шифрования)	конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования информации, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.
2.	Компьютерный вирус	программа, которая обладает следующими свойствами : возможностью копирования себя в другие файлы, диски, ЭВМ; возможностью выполнения без явного вызова; возможностью осуществления несанкционированного доступа к информации; возможностью маскировки от попыток обнаружения.
3.	Конфиденциальная информация	информация, которая представляет собой коммерческую или личную тайны и охраняется ее владельцем.
4.	Разграничение доступа	наделение каждого пользователя (субъекта доступа) индивидуальными правами по доступу к информационному ресурсу и проведению операций по ознакомлению с информацией, ее документированию, модификации и

		уничтожению. Разграничение доступа может осуществляться по различным моделям, построенным по тематическому признаку или по грифу секретности разрешенной к пользованию информации.

Критерии оценки контрольных работ ОФО:

Структура работы	Критерии оценки	Распределение баллов
Один термин (в контрольной работе каждого из модулей 4 термина)	Нет ответа / Неполный ответ / Полный ответ	0/0,5/1 за один ответ Всего: 4 балла

Темы заданий контрольных работ для ЗФО

Вариант 1
1. Понятие атрибутов доступа к файлам. Защита сетевого файлового ресурса на примерах организации доступа в различных операционных системах.
2. Понятие доступа к данным со стороны процесса; отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.
Вариант 2
1. Современные программно-аппаратные средства защиты компьютерной информации.
2. Несанкционированное копирование программ как тип несанкционированного доступа. Юридические аспекты
несанкционированного копирования программ. Способы защиты от копирования.
Вариант 3
1. Сравнительный анализ методов воздействия и противодействия в сети Internet.
2. Особенности построения защиты информации в телекоммуникационных сетях УИС.
Вариант 4
1. Методы и средства воздействия на безопасность телекоммуникационных сетей.
2. Направления по защите от враждебных воздействий на безопасность компьютерных сетей.
Вариант 5
1. Необходимые и достаточные условия предотвращения разрушающего воздействия вируса.
2. Угрозы безопасности современных информационно-вычислительных и телекоммуникационных сетей. Классификация угроз безопасности.
Вариант 6
1. Аппаратные и программно-аппаратные средства криптозащиты данных.
2. Вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий.
Вариант 7
1. Понятие атрибутов доступа к файлам. Организация доступа к файлам в различных операционных системах
2. Способы фиксации фактов доступа. Журналы доступа. Выявление следов несанкционированного доступа к файлам
Вариант 8
1. Организационно-правовая основа защиты информации в ФСИН России.
2. Методы и средства защиты данных от несанкционированного доступа.
Вариант 9
1. Понятие и содержание информационной безопасности.
2. Постановка задачи обеспечения информационной безопасности в каналах связи органов и учреждений УИС.

Вариант 10
1. Необходимость, назначение и общее содержание организационно- правового обеспечения информационной безопасности.
2. Методы и специальные технические средства, используемые в ходе поисковой операции в целях обеспечения защиты информации.
Вариант 11
1. Понятие и цели проведения специальных проверок объектов информатизации; основные этапы проведения проверки
2. Уязвимость компьютерных систем. Понятие несанкционированного доступа (НСД). Классы и виды НСД
Вариант 12
1. Основные направления инженерно-технической защиты информации: физическая защита, скрытие информации, поиск и нейтрализация источников утечки
2. Распространённые способы блокирования каналов утечки информации и виды специальных технических средств защиты
Вариант 13
1. Требования и показатели защищенности автоматизированных средств обработки информации.
2. «Типовые» каналы утечки информации объектов информатизации УИС. Условия и факторы, способствующие утечке информации ограниченного доступа.
Вариант 14
1. Методические рекомендации по обеспечению информационной безопасности связи органов и учреждений УИС.
2. Технические методы защиты информации.

Вариант 15
1. Понятие и виды каналов утечки информации. «Типовые» каналы утечки информации объектов информатизации УИС.
2. Основные угрозы безопасности информации. Общая характеристика технических средств несанкционированного получения информации и технологий их применения.
Вариант 16
1. Обеспечение безопасности ведомственной информации, информационных ресурсов, средств и систем информатизации.
2. Правовая защита сотрудников УИС от негативных информационно-психологических воздействий.
Вариант 17
1. Краткий обзор современных методов защиты информации.
2. Правовые основы защиты оперативно - розыскной информации как реализованной функции по добыванию, обработке и использованию данных и сведений.
Вариант 18
1. Обеспечение информационной безопасности в каналах связи.
2. Меры противодействия информационной безопасности в автоматизированных системах обработки данных.
Вариант 19
1. Современное состояние и перспективы развития информационной безопасности в телекоммуникационных системах информации.
2. Принципы государственной политики обеспечения
информационной безопасности Российской Федерации.

Вариант 20
1. Методы закрытия речевых сигналов в телефонных каналах связи.
2. Особенности проблем защиты конфиденциальной информации.
Вариант 21
1. Важнейшие составляющие интересов в информационной сфере и основные угрозы информационной безопасности УИС.
2. Достоверность и целостность информации при передаче по каналам связи
Вариант 22

1. Основные составляющие национальных интересов в информационной сфере; виды и источники угроз информационной безопасности Российской Федерации.
2. Назначение и краткий анализ общих моделей процесса защиты информации.

Критерии оценки контрольной работы для ЗФО

Студенту выставляется «зачтено» за выполнение контрольной работы, если даны полные и развернутые ответы по заданным терминам и определениям, а так же законам в области информационной безопасности.

Студенту выставляется «не зачтено» за выполнение контрольной работы, если не даны полные и развернутые ответы и имеются пробелы в знаниях терминов и определений в области информационной безопасности.

Комплект тестовых заданий

Модуль 1

1. Защита информации это:
   1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
   2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
   3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
   4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
   5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

2. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
   1. активный перехват;
   2. пассивный перехват;
   3. аудио-перехват;
   4. видео-перехват;
   5. просмотр мусора.

3. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
   1. активный перехват;
   2. пассивный перехват;
   3. аудио-перехват;
   4. видео-перехват;

4. Под replay-атакой понимается:
1. модификация передаваемого сообщения
2. повторное использование переданного ранее сообщения
3. невозможность получения сервиса законным пользователем

5. Уровень секретности - это
1. ответственность за модификацию и НСД информации
2. административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов

6. Что такое несанкционированный доступ (нсд)?
1. Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа

2.Создание резервных копий в организации
3. Правила и положения, выработанные в организации для обхода парольной защиты
4. Вход в систему без согласования с руководителем организации

6. К посторонним лицам нарушителям информационной безопасностиотносится:
а) персонал, обслуживающий технические средства;
б) технический персонал, обслуживающий здание;
в) сотрудники службы безопасности.
г) представители конкурирующих организаций.

8. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?
а) Безопасная OECD
2. ISO\IEC
3. OECD
4. CPTED

9. Перехват, который осуществляется путем использования оптической техники называется:
а) активный перехват;
б) пассивный перехват;
в) аудио-перехват;
г) видео-перехват;
д) просмотр мусора.

10. К внутренним нарушителям информационной безопасности относится:
а) любые лица, находящиеся внутри контролируемой территории;
б) персонал, обслуживающий технические средства.
в) сотрудники отделов разработки и сопровождения ПО;
г) технический персонал, обслуживающий здание

11. Собственником информации не может быть:
а) государство;
б) юридическое лицо;
в) группа физических лиц;
г) физическое лицо;
д) ответы а – г правильны;
е) нет правильного ответа.

12. Терминология в сфере защиты информации регулируется
а) ГОСТ Р 6.30 – 2003
б) ГОСТ 51141 – 98
в) ГОСТ 50922 – 96
г) Гражданским кодексом.

13. Заранее намеченный результат защиты информации – это
а) замысел защиты информации;
б) цель защиты информации;
в) уровень эффективности защиты информации.

14.Кто является основным ответственным за определение уровня классификации информации?
а) Руководитель среднего звена
б) Высшее руководство
в) Владелец
г) Пользователь
15.Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

Варианты ответа:
а) Сотрудники
б) Хакеры
в) Атакующие
г) Контрагенты (лица, работающие по договору)

16.Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
Варианты ответа:
а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
в) Улучшить контроль за безопасностью этой информации
г) Снизить уровень классификации этой информации

17.Что самое главное должно продумать руководство при классификации данных?
Варианты ответа:
а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
б) Необходимый уровень доступности, целостности и конфиденциальности
в) Оценить уровень риска и отменить контрмеры
г) Управление доступом, которое должно защищать данные

18.Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
а) Владельцы данных
б) Пользователи
в) Администраторы
г) Руководство

19.Что такое процедура?
а) Правила использования программного и аппаратного обеспечения в компании
б) Пошаговая инструкция по выполнению задачи
в) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
г) Обязательные действия

20.Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
Варианты ответа:
а) Поддержка высшего руководства
б) Эффективные защитные меры и методы их внедрения
в) Актуальные и адекватные политики и процедуры безопасности
г) Проведение тренингов по безопасности для всех сотрудников

21.Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
Варианты ответа:
а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
б) Когда риски не могут быть приняты во внимание по политическим соображениям
в) Когда необходимые защитные меры слишком сложны
г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

22.Что такое политики безопасности?
а) Пошаговые инструкции по выполнению задач безопасности
б) Общие руководящие требования по достижению определенного уровня безопасности
в) Широкие, высокоуровневые заявления руководства
г) Детализированные документы по обработке инцидентов безопасности

23.Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
а) Анализ рисков
б) Анализ затрат / выгоды
в) Результаты ALE
г) Выявление уязвимостей и угроз, являющихся причиной риска

24.Что лучше всего описывает цель расчета ALE?
а) Количественно оценить уровень безопасности среды

б) Оценить возможные потери для каждой контрмеры
в) Количественно оценить затраты / выгоды
г) Оценить потенциальные потери от угрозы в год

25.Тактическое планирование – это:
а) Среднесрочное планирование
б) Долгосрочное планирование
в) Ежедневное планирование
г) Планирование на 6 месяцев

Модуль 2

1.Что является определением воздействия (exposure) на безопасность?
а) Нечто, приводящее к ущербу от угрозы
б) Любая потенциальная опасность для информации или систем
в) Любой недостаток или отсутствие информационной безопасности
г) Потенциальные потери от угрозы

2.Эффективная программа безопасности требует сбалансированного применения:
а) Технических и нетехнических методов
б) Контрмер и защитных механизмов
в) Физической безопасности и технических средств защиты
г) Процедур безопасности и шифрования

3.Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
а) Внедрение управления механизмами безопасности
б) Классификацию данных после внедрения механизмов безопасности
в) Уровень доверия, обеспечиваемый механизмом безопасности
г) Соотношение затрат / выгод

4.Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?
а) Только военные имеют настоящую безопасность
б) Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
в) Военным требуется больший уровень безопасности, т.к. их риски существенно выше
г) Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

5.Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?
а) Поддержка
б) Выполнение анализа рисков
в) Определение цели и границ
г) Делегирование полномочий

6.Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
а) Чтобы убедиться, что проводится справедливая оценка
б) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
в) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
г) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

7.Что является наилучшим описанием количественного анализа рисков?
а) Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
б) Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
в) Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
г) Метод, основанный на суждениях и интуиции

8.Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

а) Стандарты
б) Должный процесс (Dueprocess)
в) Должная забота (Duecare)
г) Снижение обязательств

9.Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

а) Список стандартов, процедур и политик для разработки программы безопасности
б) Текущая версия ISO 17799
в) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
г) Открытый стандарт, определяющий цели контроля

10.Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

а) гаммирования;
б) подстановки;
в) кодирования;
г) перестановки;
д) аналитических преобразований.

11.Защита информации от утечки это деятельность по предотвращению:

а) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
б) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
в) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
г) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

12.Защита информации это:

а) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
б) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
в) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
г) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
д) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

13.Естественные угрозы безопасности информации вызваны:

а) деятельностью человека;
б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
в) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
г) корыстными устремлениями злоумышленников;
д) ошибками при действиях персонала.

14. Искусственные угрозы безопасности информации вызваны:

а) деятельностью человека;
б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
в) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
г) корыстными устремлениями злоумышленников;
д) ошибками при действиях персонала.

15. К основным непреднамеренным искусственным угрозам АСОИ относится:

а) физическое разрушение системы путем взрыва, поджога и т.п.;
б) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
в) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
г) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

16.К посторонним лицам нарушителям информационной безопасности относится:
а) персонал, обслуживающий технические средства;
б) технический персонал, обслуживающий здание;
в) представители конкурирующих организаций.
г) лица, нарушившие пропускной режим;

17.Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:
а) черный пиар;
б) фишинг;
в) нигерийские письма;
г) источник слухов;

18.Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:
а) черный пиар;
б) фишинг;
в) нигерийские письма;
г) источник слухов;

19.Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и (или) собственником информации – это
а) носитель информации
б) собственник информации
в) владелец информации
д) пользователь информации

20. Содержание и порядок действий, направленных на обеспечение защиты информации – это
а) мероприятие по защите информации;
б) система защиты информации
в) организация защиты информации.

21. В настоящее время по степени конфиденциальности можно классифицировать информацию,
а) составляющую коммерческую тайну;
б) составляющую государственную тайну;
в) составляющую служебную тайну;
г) составляющую профессиональную тайну.

22. В каких областях деятельности может быть государственная тайна
а) военной
б) образовательной
в) экономической
г) контрразведывательной
д) внешнеполитической

23.. К внутренним нарушителям информационной безопасности относится:
а) пользователи системы;.
б) персонал, обслуживающий технические средства.
в) сотрудники отделов разработки и сопровождения ПО;
г) технический персонал, обслуживающий здание

24.. Собственником информации не может быть:
а) государство;
б) юридическое лицо;
в) нет правильного ответа
г) физическое лицо;

25. Терминология в сфере защиты информации регулируется
а) ГОСТ Р 6.30 – 2003
б) ГОСТ 51141 – 98
в) ГОСТ 50922 – 96
г) Гражданским кодексом.

Критерии оценки тестовых заданий в 1 и 2 модуле ОФО

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста (25 вопросов в варианте)	Неправильный ответ / Правильный ответ	0/0,32 за один ответ Всего: 8 баллов

Критерии оценки тестовых заданий для ЗФО

60% и более правильных ответов – «зачтено»
Менее 60% правильных ответов - «не зачтено».

Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме

Интерактивное обучение – это специальная форма организации познавательной деятельности. Она подразумевает вполне конкретные и прогнозируемые цели.

Цель состоит в создании комфортных условий обучения, при которых студент или слушатель чувствует свою успешность, свою интеллектуальную состоятельность, что делает продуктивным сам процесс обучения, дать знания и навыки, а также создать базу для работы по решению проблем после того, как обучение закончится.

Интерактивное обучение – это диалоговое обучение, в ходе которого осуществляется взаимодействие между студентом и преподавателем, между самими студентами.

В рамках интерактивной лекции используются электронные образовательные ресурсы – ЭБС.

Проблемная лекция. Преподаватель в начале и по ходу изложения учебного материала создает проблемные ситуации и вовлекает студентов в их анализ. Разрешая противоречия, заложенные в проблемных ситуациях, обучаемые самостоятельно могут прийти к тем выводам, которые преподаватель должен сообщить в качестве новых знаний.

В рамках данной аудиторной работы определяются итоги освоения материала и участия студентов в дискуссии, определении проблемы и ее решении.

Критерии оценивания:

Показатель оценки	Количество баллов
Информационная готовность к аудиторной работе в интерактивной форме, умение делать выводы в проблемных ситуациях, умение найти нужную информацию, активность в обсуждении проблемы	1
ИТОГО	1

Примерные темы для круглого стола

1. Применение на практике Доктрины информационной безопасности Российской Федерации.
2. Федеральные законы в области информации и информационной безопасности.
3. Указы президента РФ и постановления правительства РФ в области информации и информационной безопасности.
4. Правовые режимы защиты информации.
5. Правовые вопросы защиты информации с использованием технических средств

Критерии и методика оценивания:

Критерии и методика оценивания:

- 5 баллов выставляется студенту, если составлен верный ответ, показано уверенное владение нормативной базой;

- 4 балла выставляется студенту, если в логическом рассуждении нет существенных ошибок; правильно сделан выбор формулировок, но допущено не более двух несущественных ошибок, получен верный ответ, нет определенной логической последовательности, неточно используется специализированная терминология;

- 3 балла выставляется студенту, если в логическом рассуждении нет существенных ошибок, но допущены существенные ошибки в выборе формулировок;

-2 балла если работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии;

- 1 балл выставляется студенту в случае, если выявлена недостаточная сформированность основных умений и навыков.

-0 баллов выставляется студенту, если студент не дал ни одного правильного ответа

Критерии оценивания для ЗФО

4 балла и более – «зачтено»

Менее 4 баллов - «не зачтено».

Типовые задания творческого уровня (доклад)

Выполняется по результатам изучения темы дисциплины с целью дополнения практического материала. Выполняется в форме доклада - представляет собой самостоятельное публичное выступление студента по представлению полученных результатов решения определенных учебно-исследовательских или научных задач Доклад готовится в интерактивной форме с соблюдение основных требований к работам такого уровня. В докладе раскрываются теоретические основы исследуемой темы, характеризуется объект исследования, выделяются основные проблемы и пути их решения.

Примеры тем творческих заданий (доклад)

1. Основные принципами обеспечения информационной безопасности в ведущих зарубежных странах.
2. Построение концепции информационной безопасности предприятия
3. Процедура аутентификации пользователя на основе пароля
4. Программная реализация криптографических алгоритмов»
5. Механизмы контроля целостности данных

Студент выбирает 2 темы для доклада из приведенного перечня.

Критерии оценки творческого задания ОФО

Показатель оценки	Распределение баллов
Соответствие содержания доклада заявленной теме, поставленным целям и задачам. Логичность и последовательность в изложении материала	1
Степень обоснованности аргументов и обобщений (полнота, глубина, всесторонность раскрытия темы, корректность аргументации и системы доказательств, характер и достоверность примеров, наличие знаний интегрированного характера, способность к обобщению). Самостоятельность изучения и анализа материала	1

Речевая культура (научный стиль изложения, владение понятийным аппаратом, четкость, лаконичность).	1
ИТОГО	3

Критерии оценивания для ЗФО

4 балла и более – «зачтено»

Менее 4 баллов - «не зачтено».

Деловая игра

1 Тема (проблема) «Безопасность в сетях», «Угрозы современных интернет -ресурсов»

2. Концепция игры.

Деловая игра – это форма воссоздания в учебном процессе предметного и социального содержания будущей профессиональной деятельности, моделирования системы отношений, характерных для информационной безопасности. В деловой игре реализуются следующие психолого-педагогические принципы: принцип имитационного моделирования условий профессиональной деятельности; принцип диалогического общения и взаимодействия участников; принцип проблемности содержания имитационной модели.

3 Роли: Каждая команда (в количестве 4-5 человек) получает проблемное задание, после выполнения которого публично защищает анкету хакера и пользователя сети.

Критерии оценки участия в деловой игре

Показатель оценки	Распределение баллов
Информационная готовность к игре (знание и понимание современных тенденций развития системы информационной безопасности, владение базовой терминологией, знание базовых нормативных актов)	1
Умение принимать управленческие решения в проблемных ситуациях (учет ограничений, наличие оригинальности в решении, отсутствие ошибок или противоречий, рациональность решений)	1
Умений работать в команде (владение навыками делового общения, самоорганизация, согласованность решений внутри группы, соблюдение деловой этики и этикета)	1
ИТОГО	3

Комплект лабораторных работ

Для самостоятельного освоения и / или расширения знаний, умений, владений предусмотрены лабораторные работы.

Лабораторная работа №1

Исследование информационной модели системы

Цель работы: Научиться основам исследования информационных систем, информационных потоков.

Ход выполнения:

Получить у преподавателя описание информационной системы. Построить IDEFмодель системы с информационными потоками.

Вопросы для контрольного опроса:

1. Что такое модель IDEF?
2. Каковы особенности взаимосвязи элементов системы?
3. Особенности композиции и декомпозиции системы.

Лабораторная работа №2

Выделение типов информации и формирование требований защиты информации

Цель работы: Научиться основам исследования информационных систем и требований к защите информационных потоков.

Ход выполнения:

По результатам лабораторной работы №1 оценить требования к информационным потокам системы. Определить требования к защите информации.

Вопросы для контрольного опроса:

1. Какие существуют угрозы для информации?
2. Как можно исключить эти угрозы?
3. Какие мероприятия применяются для устранения возможности возникновения угроз?
4. Какие мероприятия применяются для устранения последствий угроз?

Лабораторная работа №3

Разработка политик безопасности

Цель работы: Научиться основам работы с политиками безопасности.

Ход выполнения:

Создать ограничивающие политики на уровне локальных политик, политик домена, политик компьютеров, политик пользователей, политик учетных записей.

Вопросы для контрольного опроса:

1. Что такое политики безопасности?
2. Что такое локальные политики безопасности?
3. Что такое политики безопасности домена?
4. Что такое политики безопасности контроллера домена?

Лабораторная работа №4

Изучение средств защиты информации в Windows XP

Цель работы: Научиться использованию средств защиты информации.

Ход выполнения:

Для выбранных объектов установить права доступа и организовать аудит использования этих объектов

Вопросы для контрольного опроса:

1. Какие права имеются на использование файлов в Windows XP?
2. Какие права имеются на использование директорий в Windows XP?
3. Какие права имеются на использование исполняемых объектов в Windows XP?
4. Что такое аудит?
5. Какие действия с объектами можно контролировать?
6. Как организовать аудит?

Критерии оценки лабораторных работ

Показатель оценки	Распределение баллов
Точность воспроизведения учебного материала (терминов, правил, фактов, описаний, законов, методологии и т.д.)	1
Умение пользоваться первичными данными, отвечать на поставленные вопросы, формулировать выводы	1
Максимальный балл	2

Критерии и методика оценивания для ЗФО:
Подготовленная и оформленная в соответствии с требованиями лабораторная работа оценивается преподавателем по следующим критериям:
- уровень эрудированности автора по изученной теме (знание автором состояния изучаемой проблематики, знание законов и т.д.);
- логичность подачи материала, грамотность автора;
-знания и умения на уровне требований стандарта данной дисциплины: знание фактического материала, усвоение общих понятий и идей.

«не зачтено» выставляется студенту, если работа не соответствует критериям;
«зачтено» выставляется студенту, если работа полностью соответствует критериям.

4.3.Рейтинг-план дисциплины (при необходимости)

Рейтинг–план дисциплины представлен в приложении Б.

5.Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература:

1. Прохорова, О.В. Информационная безопасность и защита информации : учебник [Электронный ресурс] /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 - ISBN 978-5-9585-0603-3 Режим доступ ; http://biblioclub.ru/index.php?page=book&id=438331
2. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов [Электронный ресурс]. / В.И. Аверченков. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; Режим доступа: http://biblioclub.ru/index.php?page=book&id=93245

Дополнительная литература:

1. Голиков А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие[Электронный ресурс]Томский государственный университет систем управления и радиоэлектроники, 2015. -256с.Режим доступа //http:/http://biblioclub.ru/index.php?page=book_red&id=480636&sr=1
2. Сердюк В. А. Организация и технологии защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие[Электронный ресурс] Москва: Издательский дом Высшей школы экономики, 2015 .-574с. -Режим доступа http://biblioclub.ru/index.php?page=book_red&id=440285&sr=1

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

- Электронная библиотечная система БашГУ – www.bashlib.ru
- Электронная библиотечная система «ЭБ БашГУ» - https://elib.bashedu.ru/
- Электронная библиотечная система «Университетская библиотека онлайн» - https://biblioclub.ru/
- Электронная библиотечная система издательства «Лань» - https://e.lanbook.com/
- Автоматизированная информационная система «ДельтаБезопасность» https://sb.deltasecurity.ru
- БД периодических изданий на платформе EastView
- Научная электронная библиотека - elibrary.ru (доступ к электронным научным журналам) - https://elibrary.ru
- Справочная правовая система «КонсультантПлюс» - http://www.consultant-plus.ru

Программное обеспечение:

- Windows 8 Russian. Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Лицензия бессрочная. Договор №104 от 17.06.2013 г.
- Microsoft Office Standard 2013 Russian OLP NL AcademicEdition. Лицензия бессрочная. Договор №114 от 12.11.2014 г.

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 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус) **2. учебная аудитория для проведения занятий семинарского типа**: аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 класс деловых игр (гуманитарный корпус), аудитория № 404 (компьютерный класс) (гуманитарный корпус), аудитория № 420 (компьютерный класс) (гуманитарный корпус). **3. учебная аудитория для проведения**	**Аудитория № 404** Учебная мебель, компьютеры -15 шт. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая 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. **Аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 515**	1. Windows 8 Russian. Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Бессрочная. Договор №104 от 17.06.2013 г. 2. Microsoft Office Standard 2013 Russian OLP NL AcademicEdition. Бессрочная . Договор №114 от 12.11.2014 г. 3. КонсультантПлюс. Договор № 28826 от 09.01.2019 г. Лицензии бессрочные.

групповых и индивидуальных консультаций: аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), **4.учебная аудитория для текущего контроля и промежуточной аттестации:** аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), **5.помещения для самостоятельной работы:** аудитория № 613, читальный зал ауд.402, (гуманитарный корпус). **6.помещение для хранения и профилактического обслуживания учебного оборудования**: аудитория № 523 (гуманитарный корпус)	Учебная мебель, доска, терминал видео конференц-связи LifeSizeIcon 600-камера, интер-ая система со встроенным короткофокусным проектором PrometheanActivBoard 387 RPOMOUNTEST, профессиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMARTPodiumSP518 с ПО SMARTNotebook, матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/ThermaltakeVL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром. **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 **Читальный зал ауд.402** Учебная мебель, стенд по пожарной безопасности, моноблоки стационарные – 5 шт, принтер – 1 шт., сканер – 1 шт. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Аудитория № 523** Стол, стул, шкаф-стеллаж, мобильное мультимедийное оборудование – проектор, ноутбук, экран переносной.	

Приложение А

МИНОБРНАУКИ РОССИИ

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Информационная безопасность в профессиональной деятельности** на 8 семестр

очная форма обучения

Вид работы	Объем дисциплины
	8 семестр
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	49,2
лекций	16
практических / семинарских	16
лабораторных работ	16
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) ФКР	1,2
Учебных часов на самостоятельную работу обучающихся (СР)	6
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	52,8

Форма контроля: экзамен, 8 семестр

МИНОБРНАУКИ РОССИИ

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Информационная безопасность в профессиональной деятельности**
11 семестр

заочная форма обучения

Вид работы	Объем дисциплины	
	Курс 6, семестр 11, сессия 1	Курс 6, семестр 11, сессия 2
Общая трудоемкость дисциплины (ЗЕТ / часов)	1 ЗЕТ / 36 часов	2 ЗЕТ / 72 часа
Учебных часов на контактную работу с преподавателем:	10	3,7
лекций	4	
практических / семинарских	2	2
лабораторных работ	4	
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) ФКР		1,7
Учебных часов на самостоятельную работу обучающихся	26	60,5
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)		7,8

Форма контроля: Экзамен, 6 курс 11семестр

Для очной формы обучения

№	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	СР			
1	2	3	4	5	6	7	8	9
1	**Тема 1.Информационная безопасность как определяющий компонент национальной безопасности и экономической безопасности.** Понятие национальной безопасности: виды безопасности: государственная, экономическая, финансовая, общественная, военная, экологическая, информационная; доктрина ИБ, история проблемы ИБ, угрозы ИБ; методы и средства обеспечения ИБ; методологические и технологические основы комплексного обеспечения ИБ	2	2	4	3	Основная 1, 2 Дополнительная 1,2 http:// www.bashlib.ru	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет - источников. Выполнение практической работы, подготовка к выполнению лабораторной работ	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в круглом столе, творческое задание (доклад), лабораторная работа
2	**Тема 2. .Правовое обеспечение информационной безопасности** Законодательство РФ в области ИБ, защиты государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации; понятие и виды защищаемой информации по законодательству РФ; защита интеллектуальной собственности	2	2	4		Основная 1, 2 Дополнительная 1,2 http:// www.bashlib.ru	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет - источников. Выполнение практической работы	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в

	средствами патентного и авторского права; правовая регламентация охранной деятельности							круглом столе, творческое задание (доклад), лабораторная работа
3	**Тема 3.Организационное обеспечение информационной безопасности в профессиональной деятельности** Анализ и оценка угроз ИБ объекта; оценка ущерба вследствие противоправного раскрытия информации ограниченного доступа и меры по его локализации; средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа; служба безопасности объекта; подбор, расстановка и работа с кадрами; организация и обеспечение режима секретности	2	2			Основная 1, 2 Дополнительная 1,2 http:// www.bashlib.ru	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет - источников. Выполнение практической работы	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в круглом столе, творческое задание (доклад)
4	**Тема 4.Технические средства обеспечения информационной безопасности экономической деятельности** Общие вопросы организации противодействия технической разведке; основные организационные и технические мероприятия, используемые для противодействия технической разведке; методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам; физические основы образования побочных электромагнитных излучений от технических средств; каналы утечки информации	2	2	4		Основная 1, 2 Дополнительная 1,2 http:// www.bashlib.ru	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет - источников. Выполнение практической работы	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в круглом столе, творческое задание (доклад), лабораторная работа
5	**Тема** 5. **Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах**	2	2		3	Основная 1, 2 Дополнительная 1,2 http:// www.bashlib.ru	Самостоятельное изучение рекомендуемой	Аудиторная работа на лекционных

	Структура и принципы функционирования современных вычислительных систем. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем.						основной и дополнительной литературы, интернет - источников. Выполнение практической работы	занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в круглом столе, творческое задание (доклад)
6	**Тема 6. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств в целях обеспечения экономической безопасности** Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы. Использование простого пароля. Использование динамически изменяющегося пароля	2	2			Основная 1, 2 Дополнительная 1,2 http:// www.bashlib.ru	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет - источников. Выполнение практической работы	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в круглом столе, творческое задание (доклад)
7	**Тема 7.. Защита от компьютерных вирусов в целях обеспечения экономической безопасности** История появления компьютерных вирусов и факторы, влияющие на их распространение. Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов. Схемы заражения загрузчиков. Способы маскировки, используемые вирусами	2	2			Основная 1, 2 Дополнительная 1,2 http:// www.bashlib.ru	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет - источников. Выполнение практической работы	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в круглом столе, творческое задание (доклад)
8	**Тема 8.Современные средства защиты**	2	2	4		Основная 1, 2	Самостоятельное	Аудиторная

	информации от НСД Методы и средства ограничения доступа к компонентам ЭВМ, надежность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации, типовые решения в организации ключевых систем; защита программ от изучения, способы встраивания средств защиты в программное обеспечение					Дополнительная 1,2 http:// www. bashlib.ru	изучение рекомендуемой основной и дополнительной литературы, интернет - источников. Выполнение практической работы	работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в круглом столе, творческое задание (доклад), лабораторная работа
	Всего	16	16	16	6			

Для заочной формы обучения

№	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	СР			
1	2	3	4	5	6	7	8	9
1	**Тема 1.Информационная безопасность как определяющий компонент национальной безопасности и экономической безопасности.** Понятие национальной безопасности: виды безопасности: государственная, экономическая, финансовая, общественная, военная, экологическая, информационная; доктрина ИБ, история проблемы ИБ, угрозы ИБ; методы и средства обеспечения ИБ; методологические и технологические основы комплексного обеспечения ИБ	1	0,5	2	12	Основная 1, 2 Дополнительная 1,2 http:// www. bashlib.ru	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет - источников. Выполнение практической работы	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в круглом столе, творческое задание(доклад), лабораторная работа
2	**Тема 2. .Правовое обеспечение информационной безопасности** Законодательство РФ в области ИБ, защиты государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации; понятие и виды защищаемой информации по законодательству РФ; защита интеллектуальной собственности	1	0,5	2	12	Основная 1, 2 Дополнительная 1,2 http:// www. bashlib.ru	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет - источников. Выполнение практической работы	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в

	средствами патентного и авторского права; правовая регламентация охранной деятельности							круглом столе, творческое задание(доклад), лабораторная работа
3	**Тема 3.Организационное обеспечение информационной безопасности в профессиональной деятельности** Анализ и оценка угроз ИБ объекта; оценка ущерба вследствие противоправного раскрытия информации ограниченного доступа и меры по его локализации; средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа; служба безопасности объекта; подбор, расстановка и работа с кадрами; организация и обеспечение режима секретности	1	0,5	-	12	Основная 1, 2 Дополнительная 1,2 http:// www.bashlib.ru	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет - источников. Выполнение практической работы	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в круглом столе, творческое задание(доклад)
4	**Тема 4.Технические средства обеспечения информационной безопасности экономической деятельности** Общие вопросы организации противодействия технической разведке; основные организационные и технические мероприятия, используемые для противодействия технической разведке; методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам; физические основы образования побочных электромагнитных излучений от технических средств; каналы утечки информации	1	0,5	-	12	Основная 1, 2 Дополнительная 1,2 http:// www.bashlib.ru	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет - источников. Выполнение практической работы	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в круглом столе, творческое задание(доклад),
5	**Тема** 5. **Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах**	-	0,5	-	12	Основная 1, 2 Дополнительная 1,2 http:// www. bashlib.ru	Самостоятельное изучение рекомендуемой	Аудиторная работа на лекционных

	Структура и принципы функционирования современных вычислительных систем. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем.						основной и дополнительной литературы, интернет - источников. Выполнение практической работы	занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в круглом столе, творческое задание(доклад)
6	**Тема 6. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств в целях обеспечения экономической безопасности** Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы. Использование простого пароля. Использование динамически изменяющегося пароля	-	0,5	-	12	Основная 1, 2 Дополнительная 1,2 http:// www. bashlib.ru	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет - источников. Выполнение практической работы	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в круглом столе, творческое задание(доклад)
7	**Тема 7. Защита от компьютерных вирусов в целях обеспечения экономической безопасности** История появления компьютерных вирусов и факторы, влияющие на их распространение. Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов. Схемы заражения загрузчиков. Способы маскировки, используемые вирусами	-	0,5	-	12	Основная 1, 2 Дополнительная 1,2 http:// www. bashlib.ru	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет - источников. Выполнение практической работы	Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в круглом столе, творческое задание(доклад)
8	**Тема 8.Современные средства защиты**	-	0,5	-	12,5	Основная 1, 2	Самостоятельное	Аудиторная

	информации от НСД Методы и средства ограничения доступа к компонентам ЭВМ, надежность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации, типовые решения в организации ключевых систем; защита программ от изучения, способы встраивания средств защиты в программное обеспечение					Дополнительная 1,2 http:// www. bashlib.ru	изучение рекомендуемой основной и дополнительной литературы, интернет - источников. Выполнение практической работы	работа на лекционных занятиях, проводимых в интерактивной форме, тестирование, контрольная работа, участие в круглом столе, творческое задание(доклад)
	Всего	4	4	4	96,5			

Приложение Б

Рейтинг – план дисциплины

Информационная безопасность в профессиональной деятельности

Курс 4, семестр 8

Специальность 38.05.01 Экономическая безопасность

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Объекты информационной защиты				
Текущий контроль				20
1. Аудиторная работа на лекционных занятиях, проводимых в интерактивной форме	1	1	0	1
2. Участие в круглом столе	5	3	0	15
3. Лабораторная работа	2	2		4
Рубежный контроль				15
1.Контрольная работа	4	1	0	4
2. Творческое задание (доклад)	3	1	0	3
3. Тестирование	0,32	25	0	8
Модуль 2. Методы, способы и средства информационной безопасности				
Текущий контроль				20
1. Участие в круглом столе	5	2	0	10
2. Участие в деловой игре	3	2	0	6
3. Лабораторная работа	2	2		4
Рубежный контроль				15
3. Тестирование	0,32	25	0	8
2.Контрольная работа	4	1	0	4
3. Творческое задание (доклад)	3	1	0	3
Поощрительные баллы				
1. Участие в студенческой олимпиаде	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10
Итоговый контроль				
Экзамен	0		0	30