МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кемеровский государственный университет»
Новокузнецкий институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Кемеровский государственный университет»

Факультет информатики, математики и экономики

УТВЕРЖДАЮ:
Ректор КемГУ
_____ Просеков А.Ю.
«26» января 2019 г.

Рабочая программа дисциплины

Б1.Б.18.02 Информационная безопасность
Код, название дисциплины

Специальность
38.05.01 Экономическая безопасность

Специализация
Экономико-правовое обеспечение экономической безопасности

Уровень образования
специалитет

Квалификация
Экономист

Форма обучения
очная

Новокузнецк 2019

Сведения об утверждении:

утверждена Ученым советом факультета
(протокол Ученого совета факультета №5 от 17.01.2019)

одобрена на заседании методической комиссии
(протокол методической комиссии факультета № 5 от 17.01.2019)

одобрена на заседании обеспечивающей кафедры
(протокол № 5 от 15.01.2019) Ю.Н.Соина-Кутищева

(Ф.И.О. зав. кафедрой) / _____ *(подпись)*

Оглавление

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

В результате освоения программы специалитета обучающийся должен овладеть следующими результатами обучения по дисциплине:

Коды компетенции	**Результаты освоения ОПОП** ***Содержание компетенций***	**Перечень планируемых результатов обучения по дисциплине**
ОК-12	способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	**Знать:** - основные понятия об информации; - основы информационной и библиографической культуры; - общую характеристику процессов сбора, передачи, обработки и накопления информации, технические и программные средства реализации информационных процессов; - основы защиты информации и сведений, составляющих государственную тайну и методы защиты информации. **Уметь:** - использовать информационные системы и средства вычислительной техники в решении задач сбора, передачи, хранения и обработки экономической информации; - работать в локальных и глобальных компьютерных сетях, использовать в профессиональной деятельности сетевые средства поиска и обмена информацией; - применять информационные системы для решения задач в профессиональной деятельности с учетом основных требований информационной безопасности. **Владеть:** - методами обработки экономической информации; - методами решения экономических задач с помощью автоматизированных информационных систем. - владеть методами защиты информации
ПК-20	способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	**Знать:** - основные положения нормативных правовых актов в области защиты государственной тайны и информационной безопасности; - задачи государственных органов в рамках деятельности по обеспечению информационной безопасности; - правила засекречивания сведений, составляющих государственную тайну, порядок допуска должностных лиц и граждан к государственной тайне, правила

Коды компетенции	**Результаты освоения ОПОП** *Содержание компетенций*	**Перечень планируемых результатов обучения по дисциплине**
		пользования и обращения с секретными документами и изделиями; - правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности. **Уметь:** - соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности; - осуществлять правовые, организационные, оперативно-розыскные, информационно-аналитические, кадровые, экономические и иные меры по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления. **Владеть:** - навыками сбора и анализа материалов с целью выработки и принятия решений и мер по обеспечению режима секретности, обнаружения возможных каналов утечки сведений, представляющих охраняемую законом тайну.

2. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина реализуется в рамках базовой / вариативной части образовательной программы, является обязательной / выборной.

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 5 зачетных единиц (з.е.).

3.1. Объём дисциплины по видам учебных занятий (в часах)

Объём дисциплины	**Всего часов**
	для очной формы обучения
Общая трудоемкость дисциплины	180
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	48
Аудиторная работа:	48

Объём дисциплины	Всего часов
	для очной формы обучения
в том числе:	
лекции	16
практические занятия	32
в т.ч. в активной и интерактивной формах	16
Внеаудиторная (самостоятельная) работа обучающихся	96
Курсовое проектирование	-
Вид промежуточной аттестации обучающегося (зачет)	36

4. Содержание дисциплины, структурированное по разделам (темам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкость по видам учебных занятий (в академических часах)

№ п/п	Раздел дисциплины	Общая трудоёмкость *(часах)*	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости
			аудиторные учебные занятия		самостоятельная работа обучающихся	
		всего	лекции	практические занятия		
1.	Раздел 1. Введение в информационную безопасность	9	1	2	6	Собеседование, устный опрос, учебная задача, тест, реферат
2.	Раздел 2. Организационное обеспечение информационной безопасности	9	1	2	6	Собеседование, устный опрос, учебная задача, тест, реферат
3.	Раздел 3. Правовое обеспечение информационной безопасности	9	1	2	6	Собеседование, устный опрос, учебная задача, тест, реферат
4.	Раздел 4. Технические средства обеспечения информационной безопасности	9	1	2	6	Собеседование, устный опрос, учебная задача, тест, реферат
5.	Раздел 5. Общесистемные основы защиты	9	1	2	6	Собеседование, устный опрос, учебная задача,

№ п/п	Раздел дисциплины	Общая трудоёмкость *(часах)*	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости
			аудиторные учебные занятия		самостоятельная работа обучающихся	
		всего	лекции	практические занятия		
	информации и про-цесса ее обработки в вычислительных системах					тест, реферат
6.	Раздел 6. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	9	1	2	6	Собеседование, устный опрос, учебная задача, тест, реферат
7.	Раздел 7. Защита от компьютерных вирусов	9	1	2	6	Собеседование, устный опрос, учебная задача, тест, реферат
8.	Раздел 8. Криптографическое закрытие информации	9	1	2	6	Собеседование, устный опрос, учебная задача, тест, реферат
9.	Раздел 9. Уничтожение остаточных данных	9	1	2	6	
10.	Раздел 10. Защита от потери информации и отказов программно-аппаратных средств	9	1	2	6	
11.	Раздел 11. Защита информационно-программного обеспечения на уровне операционных систем	9	1	2	6	
12.	Раздел 12. Защита информации на уровне систем управления базами данных	9	1	2	6	
13.	Раздел 13. Специфические особенности защиты информации в локальных и глобальных	14	2	4	8	

№ п/п	Раздел дисциплины	Общая трудоёмкость *(часах)*	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости
			аудиторные учебные занятия		самостоятельная работа обучающихся	
		всего	лекции	практические занятия		
	компьютерных сетях					
14.	Раздел 14. Современные средства защиты информации от НСД	14	2	4	8	
	Всего:	180	16	32	96	

4.2 Содержание дисциплины (модуля), структурированное по темам (разделам)

Наименование раздела дисциплины	Содержание раздела дисциплины
Раздел 1. Введение в информационную безопасность	Понятие национальной безопасности: виды безопасности: государственная, экономическая, общественная, военная, экологическая, информационная; роль и место системы обеспечения информационной безопасности (ИБ) в системе национальной безопасности РФ; доктрина ИБ, история проблемы ИБ, угрозы ИБ; методы и средства обеспечения ИБ; методологические и технологические основы комплексного обеспечения ИБ
Раздел 2. Организационное обеспечение информационной безопасности	Анализ и оценка угроз информационной безопасности 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 /Лек/ Анализ и оценка угроз информационной безопасности 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;
Раздел 3. Правовое обеспечение информационной безопасности	Законодательство РФ в области информационной безопасности, 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 средствами патентного и авторского права; правовая регламентация охранной деятельности /

Раздел 4. Технические средства обеспечения информационной безопасности	Общие вопросы организации противодействия технической разведке; основные организационные и технические мероприятия, используемые для противодействия технической разведке; методы и средства защиты режимных объектов от утечки конфиденциаль-ной информации по техническим каналам; физические основы образования побочных электромагнитных излучений от технических средств; каналы утечки информации:
Раздел 5. Общесистемные основы защиты информации и про-цесса ее обработки в вычислительных системах	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. Анализ моделей нарушителя. Угрозы информационно-программному обеспечению вычислительных систем и их классификация.
Раздел 6. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	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. Взаимная проверка подлинности и другие случаи опознания. Способы разграничения доступа к компьютерным ресурсам. Разграничение
Раздел 7. Защита от компьютерных вирусов	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. Классификация компьютерных вирусов. Организация защиты от компьютерных вирусо
Раздел 8. Криптографическое закрытие информации	Введение в криптографию. Представление защищаемой информации; угрозы безопасности информации; ценность информации; основные термины и понятия криптографии; открытые сообщения и их характеристики; модели открытых сообщений; исторический очерк развития криптографии; Типы криптографических систем. Простые методы шифрования: шифры подстановки и перестановки.
Раздел 9. Уничтожение остаточных данных	Введение в проблему. Виды остаточных данных. Способы защиты от несанкционированного использования остаточной информации. Использование специализированных программ по уничтожению остаточных данных. Специальные режимы и особенности шифрования данных в режиме реального времени с возможность мгновенного уничтожения данных.
Раздел 10. Защита от потери информации и отказов программно-аппаратных средств	Основные способы защиты от потери информации и нарушений работоспособности вычислительных средств. Внесение функциональной и информационной избыточности. Способы резервировании информации. Правила обновления резервных данных. Методы сжатия информации. Архивация файловых данных. Особенности архивации на магнитные диски и магнитную ленту. Резервирование системных данных. Подготовка программных средств
Раздел 11. Защита информационно-программного обеспечения на уровне	Общие сведения о реализации защиты информационно-программного обеспечения в операционных системах. Классификация функций защиты по уровням безопасности, поддерживаемых операционной системой (ОС). Ядро безопасности ОС. Аппаратная осно-ва реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС. Внесение функциональной и

операционных систем	информационной избыточности ресурсов на уровне ОС.
Раздел 12. Защита информации на уровне систем управления базами данных	Концептуальные вопросы построения уровней защиты систем управления базами данных (СУБД). Основные требования к подсистеме безопасности СУБД. Общие сведения о разграничении доступа к базам данных. Обязанности администратора по защите баз данных от несанкционированного доступа. Определение полномочий пользователей по доступу к базе данных. /Лек/
Раздел 13. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности. Угрозы информационно-программному обеспечению, характерные только для распределенной вычислительной среды. Использование криптографических систем для защиты данных, циркулирующих в вычислительной сети. Особенности применения симметрических и асимметрических систем шифрования.
Раздел 14. Современные средства защиты 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

Содержание практических занятий

Номер раздела дисциплины	**Темы практических занятий**
1	Защта ПК на уровне BIOS
2	Защита от компьютерных вирусов
3	Использование общесисистемных и специализированных программныз средств для шифрования файлов
4	Использование специализированных программ по уничтожению остаточных данных
5	Резервирование системных данных
6	Защита ОС Windows
7	Защита баз данных
8	Защита в Internet и Intranet

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Самостоятельная работа обучающегося по дисциплине предполагает: систематизацию и закрепление полученных теоретических знаний и практических умений; углубление и расширение теоретических знаний; формирование умений использовать полученные знания; развитие познавательных способностей и активности студента; формирование самостоятельности мышления; способности к самообразованию и саморазвитию; формирование практических навыков и умений; повышение мотивации студента к научно-познавательной деятельности.

Учебный процесс по дисциплине включает два вида самостоятельной работы: аудиторную и внеаудиторную.

Самостоятельная работа студента по дисциплине включает в себя: подготовку к аудиторным занятиям (лекция, практическим) и выполнение заданий по темам дисциплины; самостоятельную работу по отдельным темам дисциплины в соответствии с рабочей программой; выполнение письменных работ; подготовку к промежуточной аттестации.

Учебно-методическое обеспечение включает в себя перечень основной и дополнительной литературы, фонд оценочных средств по дисциплине.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

6.1. Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции (или её части) / и ее формулировка	Наименование оценочного средства
1.	Раздел 1. Введение в информационную безопасность	ОК-12, ПК-20	Собеседование, устный опрос, учебная задача, комплексная ситуационная задача, тест, реферат
2.	Раздел 2. Организационное обеспечение информационной безопасности	ОК-12, ПК-20	Собеседование, устный опрос, учебная задача, комплексная ситуационная задача, тест, реферат
3	Раздел 3. Правовое обеспечение информационной безопасности	ОК-12, ПК-20	Собеседование, устный опрос, учебная задача, комплексная ситуационная задача, тест, реферат
4	Раздел 4. Технические средства обеспечения информационной безопасности	ОК-12, ПК-20	Собеседование, устный опрос, учебная задача, комплексная ситуационная задача, тест, реферат
5	Раздел 5. Общесистемные основы защиты информации и про-цесса ее обработки в вычислительных системах	ОК-12, ПК-20	Собеседование, устный опрос, учебная задача, комплексная ситуационная задача, тест, реферат
6	Раздел 6. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	ОК-12, ПК-20	Собеседование, устный опрос, учебная задача, комплексная ситуационная задача, тест, реферат
7	Раздел 7. Защита от компьютерных вирусов	ОК-12, ПК-20	Собеседование, устный опрос, учебная задача, комплексная ситуационная задача, тест, реферат
8	Раздел 8. Криптографическое закрытие информации	ОК-12, ПК-20	Собеседование, устный опрос, учебная задача, комплексная ситуационная задача, тест, реферат
9	Раздел 9. Уничтожение остаточных данных	ОК-12, ПК-20	Собеседование, устный опрос, учебная задача, комплексная ситуационная задача, тест, реферат

№ п/п	Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции (или её части) / и ее формулировка	Наименование оценочного средства
	Раздел 10. Защита от потери информации и отказов программно-аппаратных средств	ОК-12, ПК-20	Собеседование, устный опрос, учебная задача, комплексная ситуационная задача, тест, реферат
	Раздел 11. Защита информационно-программного обеспечения на уровне операционных систем	ОК-12, ПК-20	Собеседование, устный опрос, учебная задача, комплексная ситуационная задача, тест, реферат
	Раздел 12. Защита информации на уровне систем управления базами данных	ОК-12, ПК-20	Собеседование, устный опрос, учебная задача, комплексная ситуационная задача, тест, реферат
	Раздел 13. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	ОК-12, ПК-20	Собеседование, устный опрос, учебная задача, комплексная ситуационная задача, тест, реферат
	Раздел 14. Современные средства защиты информации от НСД	ОК-12, ПК-20	Собеседование, устный опрос, учебная задача, комплексная ситуационная задача, тест, реферат

6.2. Типовые контрольные задания или иные материалы

6.2.1. Экзамен

а) типовые вопросы (задания):

1 Правовое регулирование в области безопасности информации: законодательная база информатизации общества; структура государственных органов, обеспечивающих безопа-ность информационных технологий.
2 Информационная безопасность. Основные определения.
3 Угрозы информационной безопасности.
4 Модель системы зашиты.
5 Организационные меры и меры обеспечения физической безопасности.
6 Идентификация и аутентификация. Методы аутентификации.
7 Особенности парольных систем аутентификации: рекомендации по практической реализации парольных систем, оценка стойкости парольных систем, методы хранения паролей.
8 Методы разграничения доступа. Криптографические методы обеспечения конфиденциальности информации.
9 Методы зашиты внешнего периметра.
10 Системы обнаружения вторжений (Intrusion Detection System, EDS)
11 Протоколирование и аудит.
12 Построение систем защиты от угроз нарушения целостности: типовая структура такой системы.
13 Криптографические методы обеспечения целостности информации: реализация меха-низма цифровой подписи, криптографические хэш-функции и ее преимущества, коды проверки

подлинности.
14 Структура системы защиты от угроз нарушения доступности: поясните основные составляющие.
15 Формальные модели управления доступом: модель Харрисона-Руззо-Ульмана, модель Беллл-ЛаПалулы.
16 Формальные модели целостности: .модель Кларка-Вилсона, модель Биба.
17 Основные положения ISO/IEC 15408. Критерии оценки безопасности информацион-ных технологий. Понятия безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-2002. Структура профиля защиты в соответствии с ГОСТ Р ИСО/МЭК 15408-2002
18 Основные положения ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью"
19 Основные положения ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования". Этапы построения и использования СМИБ
20 Обобщенная схема построения комплексной защиты компьютерной сети предприятия на примере модели Lifecycle Security.
21 Технология функционирования VPN. Типы виртуальных частных сетей, преимуще-ства и недостатки.
22 Методика анализа рисков в сфере информационной безопасности CRAMM
23 Методика анализа рисков в сфере информационной безопасности FRAP
24 Методика анализа рисков в сфере информационной безопасности OCTAVE
25 Методика анализа рисков в сфере информационной безопасности RiskWatch
26 Проведение оценки рисков в соответствии с методикой Microsoft
27 Опишите суть протокола системы централизованной аутентификации и распределе-ния ключей симметричного шифрования Kerberos Протоколы и механизмы обеспечения информационной безопасности Kerberos, S/MIME, IPSec, AH, ESP, IPSec, NAT. Опишите их назначение и область применения.

Темы письменных работ

Эффективность защиты информации
Защита ПК от программных закладок
Парольная защита ОС UNIX
Парольная защита ОС Linux
Парольная защита ОС Windows 95/98
Парольная защита ОС Windows NT
Парольная защита ОС Windows XP
Восстановление информации на жестком дике
Защита ПК от компьютерных вирусов
Криптографические методы защиты информации
Криптогафические протоколы
Надежность криптосистем
Защита ПК от несанкционированного доступа
Технические средства обеспечения информационной безопасности
Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств
Защита информации на уровне систем управления базами данных
Защита информации в локальных компьютерных сетях
Защита информации в глобальных компьютерных сетях
Файловые системы жестких дисков
Диагностирование и устранение логических и физических дефектов магнитных дисков

б) критерии оценивания компетенций (результатов), описание шкалы оценивания:

Критерии и шкала оценивания компетенций

Результаты зачета оцениваются как **«зачтено»** и **«не зачтено»**. При выставлении оценок учитывается уровень приобретенных компетенций студента по составляющим «знать», «уметь», «владеть». Компонент «знать» оценивается теоретическими вопросами по содержанию дисциплины в ходе зачета. Компоненты «уметь» и «владеть» оцениваются практико-ориентированными заданиями, выполненными в течение семестра в соответствии с паспортом оценочных средств. Большое значение имеют объем, глубина знаний, аргументированность и доказательность умозаключений студента, а также общий кругозор студента.

При выставлении оценки преподаватель руководствуется следующим:

Оценка **«зачтено»** выставляется студенту, если дан ответ на теоретический вопрос и выполнено практикоориентированное задание. Содержание ответов свидетельствует о базовых знаниях студента по дисциплине и о его умении решать профессиональные задачи, соответствующие его будущей квалификации.

Оценка **«незачтено»** выставляется студент, если не дан ответ на теоретический вопрос или не выполнено практикоориентированное задание, а также, если содержание ответов свидетельствует об отсутствии базовых знаний студента по дисциплине и о его неумении решать профессиональные задачи.

При выставлении оценки экзаменатор руководствуется следующим:

- **«отлично»** - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений,

- **«хорошо»** - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

- **«удовлетворительно»** - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;

- **«неудовлетворительно»** - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач.

6.2.2. Текущий контроль

Оценочные средства для осуществления текущего контроля по дисциплине содержатся в Фонде оценочных средств.

Критерии оценивания знаний, умений и навыков студентов при проведении текущего контроля с использованием различных оценочных средств представлены ниже.

А) Собеседование и устный опрос

Аналитическая шкала оценивания ответов на устные вопросы

Уровни / критерии	***Недостаточный уровень***	***Базовый уровень (1 балл)***	***Повышенный уровень (2 балла)***
Полнота раскрытия вопроса	Вопрос не раскрыт либо ответ основан на недостоверной информации, выступающим допущены принципиальные ошибки при изложении материала.	Вопрос раскрыт, отвечающий ясно и грамотно излагает материал, основываясь на учебной литературе, владеет необходимой терминологией	Ответ содержит полную информацию по вопросу, основанную на учебной и дополнительной специальной литературе, ответ сопровождается демонстрационным материалом

Б) Учебная задача и комплексная ситуационная задача

Аналитическая шкала оценивания решения учебных задач

Уровни / критерии	***Недостаточный уровень***	***Базовый уровень (1 балл)***	***Повышенный уровень (2 балла)***
Самостоятельность выполнения задания	Помощь преподавателя требовалась постоянно	Помощь преподавателя требовалась иногда	Помощь преподавателя не требовалась
Детальность анализа ситуации, изложенной в казусе	Не проведен анализ ситуации, изложенной в казусе	Проведен общий анализ ситуации, изложенной в казусе	Проведен детальный анализ ситуации, изложенной в казусе с подробной характеристикой её элементов
Полнота и обоснованность сделанных выводов	Выводы по задаче не сделаны	Сделан общий вывод по задаче	Сделан детальный и обоснованный вывод по задаче

В) Тест

Критерии оценивания теста

Тест рубежного контроля включает от 10 до 30 заданий. Верное выполнение каждого задания оценивается в 0,5 балла. За неверный ответ или отсутствие ответа выставляется 0 баллов. Частично правильные ответы на задание не предусмотрены. Общий тестовый балл определяется суммой баллов, полученных за верное выполнение заданий теста. Время тестирования - 1,5 минуты на одно задание.

Г) Реферат

Реферат - это индивидуальная научно-исследовательская работа студента. При выполнении реферата необходимо раскрыть суть исследуемой проблемы с различных позиций и точек зрения, сформулировать самостоятельные выводы.

Критерии оценивания реферата

Реферат оценивается преподавателем по зачетной системе исходя из следующих критериев:

- степень освещенности теоретического вопроса;
- использование специальной научной литературы;
- творческий подход к разработке темы;
- правильность и научная обоснованность выводов;
- аккуратность оформления.

Реферат не зачитывается, если: выполнен не по соответствующей теме; базируется на устаревших источниках; тождественен реферату другого студента; не раскрывает существа темы.

Если представленный реферат не отвечает установленным требованиям, он возвращается студенту. Преподаватель отмечает недостатки и дает рекомендации по их устранению.

6.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Порядок оценки учебной деятельности студентов по дисциплине осуществляется в соответствии с Положением «О балльно-рейтинговой системе оценки деятельности обучающихся КемГУ» от 30 декабря 2015 г.

Комбинация различных оценочных мероприятий и баллов представлена в таблице рейтинг-плана.

Рейтинг-план дисциплины

№	*Контрольные мероприятия и средства оценивания*	*Кол-во баллов за конкретное задание*	*Кол-во мероприятий за семестр*	*Максимальное количество баллов*
1	Виды оценочных средств, используемых на практических занятиях:			
1.1	Ответ на устный вопрос, участие в дискуссии	2	10	20
1.2	Решение учебной или ситуативной задачи	3	10	30
1.3	Тестирование	10	3	30
1.4	Участие в деловой игре или в иных мероприятиях, проводимых в интерактивной форме	5	1	5
Виды оценочных средств, используемых для контроля самостоятельной работы:				
2	Реферат	5	1	5
3	Научный доклад, заслушанный на научной студенческой секции или научно-практической	10	1	10

	конференции			

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

Основная литература

1. Шаньгин, В. Ф. Информационная безопасность [Электронный ресурс] : учеб. пособие / В. Ф. Шаньгин. - Электронные текстовые данные. - Москва : ДМК Пресс, 2014. – 702 с. - Режим доступа: https://e.lanbook.com/book/50578

Дополнительная литература

1.Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. – Электронные текстовые данные. - Москва : РИОР, 2013. – 222 с. - Режим доступа: http://znanium.com/bookread2.php?book=405000

2.Веселов, Г. Е. Менеджмент риска информационной безопасности [Электронный ресурс] : учеб. пособие / Г. Е. Веселов, Е. С. Абрамов, А. К. Шилов ; Министерство образования и науки РФ, Южный федеральный университет, Инженерно-технологическая академия. - Электронные текстовые данные. - Таганрог : Издательство Южного федерального университета, 2016. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=493331

3. Внуков, А. А. Защита информации в банковских системах [Электронный ресурс] : учеб. пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Электронные текстовые данные. - Москва : Юрайт, 2018. — 246 с. — (Серия : Бакалавр и магистр. Академический курс). – Режим доступа: https://biblio-online.ru/book/zaschita-informacii-v-bankovskih-sistemah-414083

4.Основы информационной безопасности [Электронный ресурс] : учеб. пособие / Е. Б. Белов [и др.]. – Электронные текстовые данные. - Москва : Горячая линия-Телеком, 2011. - Режим доступа: https://e.lanbook.com/book/111016

5.Петров, В. П. Информационная безопасность человека и общества [Текст] : учеб. пособие для вузов / В. П. Петров, С. В. Петров. - Москва : ЭНАС, 2007. - 333 с.

8. Перечень ресурсов сети «Интернет», необходимых для освоения дисциплины

1. http://www.garant.ru/ – Система «Гарант», правовые базы российского законодательства.
2. http://www.consultant.ru/ - Общероссийская сеть распространения правовой информации (Консультант-плюс).
3. www.pravo.ru - Справочно-правовая система (раздел «Судебная база»).
4. www.rg.ru – сервер «Российской газеты» - официального источника опубликования федеральных законов и иных нормативных правовых актов.

9. Методические указания для обучающихся по освоению дисциплины

А) Методические рекомендации по освоению лекционного материала, подготовке к лекциям

С целью успешного освоения лекционного материала по дисциплине рекомендуется осуществлять его конспектирование.

Механизм конспектирования лекции составляют:

- восприятие смыслового сегмента речи лектора с одновременным выделением значимой информации;
- выделение информации с ее параллельным свертыванием в смысловой сегмент;
- перенос смыслового сегмента в знаковую форму для записи посредством выделенных опорных слов;
- запись смыслового сегмента с одновременным восприятием следующей информации.

Б) Методические рекомендации по подготовке к практическим занятиям

Подготовка к практическим занятиям включает в себя изучение рекомендованной учебной и специальной литературы.

При подготовке к ответу на теоретические вопросы необходимо уяснить содержание и значение основных понятий и категорий дисциплины. Большую помощь при изучении дисциплины может оказать знакомство с публикациями в рекомендованных преподавателем журналах.

К ответам студентов на вопросы по дисциплине предъявляются следующие требования:

- четко сформулируйте проблему, которую необходимо раскрыть;
- изложите свою точку зрения на рассматриваемый вопрос, аргументируйте ее, подкрепите соответствующим материалом, ссылками на источники;
- сделайте выводы, которые вытекают из сказанного;
- запишите заключение, сделанное преподавателем в конце занятия.

Решать практические задачи рекомендуется в следующей последовательности:

1. внимательно прочитать условие задачи;
2. определить знание, каких институтов позволит ответить на поставленные вопросы;
3. сформулировать выводы по задаче, подкрепив их ссылками на источники.

Решение задачи рекомендуется записывать в специально отведенную для этих целей тетрадь.

В) Методические рекомендации по организации самостоятельной работы

Вся учебная деятельность студента – это различные виды, формы и уровни самостоятельной работы, поэтому она является ведущей формой обучения в вузе.

Аудиторная самостоятельная работа проводится в ходе: 1) лекционных занятий; 2) практических занятий.

Самостоятельная работа студентов на лекции включает в себя умение слушать внимательно, выделять тезисы, которые составляют основу излагаемых проблем и логику доказательств основных положений изучаемой темы, выделять главное в содержании лекции, конспектировать.

Результатом самостоятельной работы студентов на лекционном занятии является написание конспекта лекции. Конспект лекции по дисциплине может включать основные блоки материла, проблемные вопросы к ним, ссылки на источники. Специфика конспектирования лекции заключается в особенностях обработки получаемой информации, в ее свертывании, что позволяет позднее восстановить коммуникативно-информационный процесс лекционного занятия.

Конспект лекции позволяет не только возвращаться к воспринятой ранее информации, но и совершенствовать ее, использовать на практике, расширять в ходе работы с рекомендованными нормативными актами и литературой. Конспект лекции позволяет хранить систему знаков, стимулирующих развертывание полученной информации.

После лекции самостоятельная работа студентов заключается в последующей работе над содержанием лекции (заметки на полях), понятиями, составлением собственного плана изучения явления.

К традиционным формам самостоятельной работы на практическом занятии относится: работа с текстами источников, заполнение таблиц, контрольные работы, развернутое оппонирование по теоретическим сообщениям, тестовые занятия различных уровней, вопросы для самопроверки.

К специфическим формам самостоятельной работы на практических занятиях по дисциплине относится: решение практических задач и казусов; реферативный обзор статей в журналах; подбор примеров и моделирование различных практических ситуаций.

Для проверки результатов самостоятельной работы используются следующие формы контроля: 1. Устные опросы и собеседования на практических занятиях; 2. Проверка решения учебных задач и комплексных ситуативных заданий (в устной форме на практическом занятии); 3. Проверка результатов тестов; 4. Заслушивание докладов и проверка рефератов.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При осуществлении образовательного процесса по дисциплине используются такие информационные технологии как:

1. Проведение лекций с использованием электронного конспекта слайд-презентаций.
2. При подготовке к практическим занятиям используются учебные материалы, размещенные в электронных библиотечных системах, доступ к которым с компьютеров НФИ КемГУ является свободным, а с домашних компьютеров – авторизированным.

1.Электронно-библиотечная система "Лань"» - http://e.lanbook.com Договор № 13-ЕП от 29.03.2018 г.

2. Электронно-библиотечная система «Знаниум» - www.znanium.com Договор № 44/2017 от 21.02.2017 г., Доп. соглашение №1 от 01.02.2018 г.

3. Электронно-библиотечная система «Университетская библиотека онлайн» (базовая часть) - http://biblioclub.ru. Контракт № 003-01/18 от 19.02.2018 г.

4.Электронно-библиотечная система «Юрайт» - www.biblio-online.ru. Договор № 53/2018 от 19.02.2018 г.

5. Межвузовская электронная библиотека (МЭБ) - https://icdlib.nspu.ru Договор о присоединении к МЭБ от 15.10.2013 г., бессрочный.

6. Электронная полнотекстовая база данных периодических изданий по общественным и гуманитарным наукам ООО «ИВИС», https://dlib.eastview.com,

Договор № 180-П от 18.10.2018 г. Доступ к периодическим изданиям 2019 г. и архив за предыдущие годы.

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Освоение дисциплины производится на базе лекционных учебных аудиторий НФИ КемГУ, обеспеченных мультимедийным оборудованием. Для проведения лекций по всем разделам курса необходим компьютер с прикладным программным обеспечением и периферийными устройствами: проектор; колонки; средства для просмотра презентаций MS PowerPoint; программа для просмотра видео файлов.

Для дисциплины предусмотрены:

Лаборатория экономического анализа и бухгалтерского учета (№ 509)

– проектор Sony VPL-ES – 1 шт.;
– экран настенный IProJectaI - 1 шт.;
– ПК на базе процессора Amd 6300-3,70Ghz/ монитор Benq; с выходом в Интернет – 19 шт.;
– кондиционер LG стационарная сплит-система - 1 шт.;
– специализированное программное обеспечение "1С: Предприятие"
– программный комплекс «ИНЭК – Аналитик»

12. Иные сведения и (или) материалы

12.1.Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для обеспечения образования инвалидов и лиц с ограниченными возможностями здоровья преподавателем дисциплины разрабатываются адаптированные задания и дополнительные наглядные материалы с учётом особенностей их психофизического развития и состояния здоровья.

Составитель (и): _____
(*фамилия, инициалы и должность преподавателя (ей)*)