МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
ИМЕНИ И. Т. ТРУБИЛИНА»**

ЭКОНОМИЧЕСКИЙ ФАКУЛЬТЕТ

УТВЕРЖДАЮ
Декан экономического
факультета
_____
профессор К. Э. Тюпаков
23 марта 2020 г.

Рабочая программа дисциплины

Информационная безопасность

Специальность
38.05.01 Экономическая безопасность

Специализация
«Экономико-правовое обеспечение экономической безопасности»

Уровень высшего образования
специалитет

Форма обучения
очная и заочная

Краснодар
2020

Рабочая программа дисциплины «Информационная безопасность» разработана на основе ФГОС ВО 38.05.01 Экономическая безопасность, утвержденного приказом Министерства образования и науки РФ 16 января 2017 г. № 20

Автор
канд. техн. наук, доцент _____ В. Н. Лаптев

Рабочая программа обсуждена и рекомендована к утверждению решением кафедры компьютерных технологий и систем от 16.03.2020 г., протокол № 7

Заведующий кафедрой
д-р техн. наук, профессор _____ В. И. Лойко

Рабочая программа одобрена на заседании методической комиссии экономического факультета, протокол от 23.03.2020 г. № 17.

Председатель
методической комиссии
д-р экон. наук, профессор _____ А. В. Толмачев

Руководитель
основной профессиональной
образовательной программы
д-р экон. наук, профессор _____ А. Б. Мельников

1 Цель и задачи освоения дисциплины

Целью освоения дисциплины «Информационная безопасность» является формирование комплекса знаний об организационных, научных и методических основах информационной безопасности (ИБ), освоение методов анализа процессов, происходящих в сфере ИБ; изучение принципов ее функционирования и развития и использование полученных результатов в экономико-правовом обеспечении экономической безопасности(ЭБ) предприятий и отраслей.

Задачи дисциплины

– раскрыть особенности функционирования ИБ экономических систем, их структур и динамики развития;

– ознакомить обучающихся с основными видами и структурами связей элементов систем ИБ, механизмами ее устойчивого функционирования и развития;

– раскрыть факторы, воздействующие на функционирование и развитие ИБ в экономико-правовое обеспечение экономической безопасности предприятий, национальных и мировой экономик в целом, при их взаимодействиях и интеграции.

2 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

В результате освоения дисциплины формируются следующие компетенции:

ОК-12 способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи 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;

ПСК-1 - способностью сбора и обработки информации о финансово-хозяйственной деятельности субъектов хозяйствования различных организационно-правовых форм и отраслевой принадлежности, в том числе в АПК; выявлять взаимосвязь и взаимозависимость экономических и правовых аспектов при раскрытии преступлений в сфере экономики.

3 Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность» является дисциплиной базовой части ОПОП ВО подготовки обучающихся по специальности 38.05.01 Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности».

4 Объем дисциплины(108 часов, 3 зачетные единицы)

Виды учебной работы	Объем, часов	
	Очная	Заочная
Контактная работа в том числе: — аудиторная по видам учебных занятий	**35** 34	**11** 10
— лекции	18	4
— лабораторные	16	6
— внеаудиторная	1	1
— зачет	1	1
Самостоятельная работа	**73**	**97**
Итого по дисциплине	**108**	**108**

5 Содержание дисциплины

По итогам изучаемой дисциплины обучающиеся сдают зачет.

Дисциплина изучается: на 4 курсе, в 7 семестре очной формы обучения, на 4 курсе, в 7 семестре заочной формы обучения.

Содержание и структура дисциплины по очной форме обучения

№ п/п	Тема. Основные вопросы	Формируемые компетенции	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)		
				Лекции	Лабораторные занятия	Самостоятельная работа
1	Объект и предмет защиты. 1.1 Угрозы и концепция ИБ. 1.2 Цели и задачи дисциплины. 1.3 Направления обеспечения ИБ	ОК-12, ПК-20, ПСК-1	7	2	2	7
2	Системы защиты информации (СЗИ) от случайных угроз, традиционного шпионажа и диверсий. 2.1 Классификация угроз 2.2 Случайные угрозы 2.3 Преднамеренные угрозы	ОК-12, ПК-20, ПСК-1	7	2	2	7

№ п/п	Тема. Основные вопросы	Формируемые компетенции	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)		
				Лекции	Лабораторные занятия	Самостоятельная работа
3	СЗИ от побочных электромагнитных излучений и наводок (ПЭМИН) 3.1 Методы защиты от ПЭМИН 3.2 Средства выявления и защиты от ПЭМИН 3.3 Активные методы защиты от ПЭМИН	ОК-12, ПК-20, ПСК-1	7	2	2	7
4	Защита информации (ЗИ) от несанкционированного доступа (НСД) 4.1 Общие требования к защищенности от НСД 4.2 Защита от закладок программных и аппаратных закладок 4.3 Защита от несанкционированного изменения структур	ОК-12, ПК-20, ПСК-1	7	2	2	7
5	Компьютерные вирусы и механизмы борьбы с ними. 5.1 Классификация компьютерных вирусов (КВ) 5.2 Принципы и методы защиты от КВ 5.3 Профилактика заражений КВ АИС	ОК-12, ПК-20, ПСК-1	7	2	2	7
6	Принципы применения криптографической ЗИ. 6.1 Классификация методов криптографического преобразования информации 6.2 Стандарты шифрования 6.3 Перспективы использования шифрования в АИС	ОК-12, ПК-20, ПСК-1	7	2	2	7
7	Программно-аппаратные средства шифрования 7.1 Системы криптографической защиты данных на основе плат "КРИПТОН". 7.2 .Защита данных от изменений 7.2 Защита файлов от изменений	ОК-12, ПК-20, ПСК-1	7	2	1	7
8	ЗИ в распределенных компьютерных системах (РКС). 8.1 Архитектура РКС 8.2 Обеспечение ИБ в пользовательской подсистеме и специализированных РКС 8.3 ЗИ на уровне подсистем управления РКС	ОК-12, ПК-20, ПСК-1	7	2	1	8
9	Особенности защиты информации в РКС. 9.1 Концепция создания защищенных КС 9.2 Методологи проектирования КСЗИ 9.3 Этапы создания компьютерных систем ЗИ (КСЗИ)	ОК-12, ПК-20, ПСК-1	7	2	1	8
10	Теория КСЗИ. 10.1 Математическая постановка задачи разработки КСЗИ 10.2 Моделирование и реализация КСЗИ 10.3 Техническая эксплуатация КСЗИ	ОК-12, ПК-20, ПСК-1	7	-	1	8
Итого				**18**	**16**	**73**

Содержание и структура дисциплины по заочной форме обучения

№ п / п	Тема. Основные вопросы	Формируемые компетенции	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)		
				Лекции	Лабораторные занятия	Самостоятельная работа
1	Объект и предмет защиты. 1.1 Угрозы и концепция ИБ. 1.2 Цели и задачи дисциплины. 1.3 Направления обеспечения ИБ	ОК-12, ПК-20, ПСК-1	7	1	1	5
	Системы защиты информации (СЗИ) от случайных угроз, традиционного шпионажа и диверсий. 2.1 Классификация угроз 2.2 Случайные угрозы 2.3 Преднамеренные угрозы	ОК-12, ПК-20, ПСК-1	7			
2	СЗИ от побочных электромагнитных излучений и наводок (ПЭМИН) 3.1 Методы защиты от ПЭМИН 3.2 Средства выявления и защиты от ПЭМИН 3.3 Активные методы защиты от ПЭМИН	ОК-12, ПК-20, ПСК-1	7		1	10
3	Защита информации (ЗИ) от несанкционированного доступа (НСД) 4.1 Общие требования к защищенности от НСД 4.2 Защита от закладок программных и аппаратных закладок 4.3 Защита от несанкционированного изменения структур.	ОК-12, ПК-20, ПСК-1	7	1		9
4	Компьютерные вирусы и механизмы борьбы с ними. 5.1 Классификация компьютерных вирусов (КВ) 5.2 Принципы и методы защиты от КВ 5.3 Профилактика заражений КВ АИС	ОК-12, ПК-20, ПСК-1	7	-	1	10
5	Компьютерные вирусы и механизмы борьбы с ними. 5.1 Классификация компьютерных вирусов (КВ) 5.2 Принципы и методы защиты от КВ 5.3 Профилактика заражений КВ АИС	ОК-12, ПК-20, ПСК-1	7	1		9
6	Принципы применения криптографической ЗИ. 6.1 Классификация методов криптографического преобразования информации 6.2 Стандарты шифрования 6.3 Перспективы использования шифрования в АИС	ОК-12, ПК-20, ПСК-1	7		1	10
7	Программно-аппаратные средства шифрования 7.1 Системы криптографической защиты данныхна основе плат "КРИПТОН".	ОК-12, ПК-20, ПСК-1	7	-		10

№ п/п	Тема. Основные вопросы	Формируемые компетенции	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)		
				Лекции	Лабораторные занятия	Самостоятельная работа
	7.2 .Защита данных от изменений 7.2 Защита файлов от изменений					
8	ЗИ в распределенных компьютерных системах (РКС). 8.1 Архитектура РКС 8.2 обеспечение ИБ в пользовательской подсистеме и специализированных РКС 8.3 ЗИ на уровне подсистем управления РКС	ОК-12, ПК-20, ПСК-1	7	1	1	10
9	Особенности защиты информации в РКС. 9.1 Концепция создания защищенных КС 9.2 Методологи проектирования КСЗИ 9.3 Этапы создания компьютерных систем ЗИ (КСЗИ)	ОК-12, ПК-20, ПСК-1	7	-	1	9
10	Теория КСЗИ. 10.1 Математическая постановка задачи разработки КСЗИ 10.2 Моделирование и реализация КСЗИ 10.3 Техническая эксплуатация КСЗИ	ОК-12, ПК-20, ПСК-1	7	-	-	11
Итого				**4**	**6**	**97**

6 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Методические указания (для самостоятельной работы)

1. Информационная безопасность: метод. рекомендации по организации самостоятельной работы студентов, обучающихся по специальности 38.05.01 Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности»/ сост.: В. Н. Лаптев. – Краснодар: КубГАУ, 2020. – 31 с. Режим доступа: https://edu.kubsau.ru/file.php/118/_38.05.01_EHB_IB_MU_po_org_SR_Laptev_Melnikov_Snimshchikova_2020_570174_v1_.PDF

2.Информационная безопасность: Практикум для студентов. – /В. И. Лойко., В. Н. Лаптев. – Краснодар: КубГАУ, – 128с. (в электронном виде на кафедре КТС).

7 Фонд оценочных средств для проведения промежуточной аттестации

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП ВО

Номер семестра	Этапы формирования и проверки уровня сформированности компетенций по дисциплинам, практикам в процессе освоения ОПОП ВО
ОК-12 способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	
4, 3	Статистика
5	Информационные системы в экономике
7	*Информационная безопасность*
8	Криминалистика
9	Методика расследований преступлений в сфере экономики
А	Защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты
ПК-20 способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	
1	Экономическая информатика
5	Исследование операций
7	*Информационная безопасность*
8	Практика по получению профессиональных умений и опыта профессиональной деятельности
А	Защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты
ПСК-1- способностью сбора и обработки информации о финансово- хозяйственной деятельности субъектов хозяйствования различных организационно-правовых форм и отраслевой принадлежности, в том числе в АПК; выявлять взаимосвязь и взаимозависимость экономических и правовых аспектов при раскрытии преступлений в сфере экономики	
5	Основы предпринимательства
7	*Информационная безопасность*
8	Экономика отраслей агропромышленного комплекса
8	Практика по получению профессиональных умений и опыта профессиональной деятельности
9	Судебная экономическая экспертиза
А	Внешнеэкономическая деятельность
А	Защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Планируемые результаты освоения компетенции (индикаторы достижения компетенции)	Уровень освоения				Оценочное средство
	неудовлетворительно (минимальный)	удовлетворительно (пороговый)	хорошо (средний)	отлично (высокий)	
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 методы и средства поиска, систематизации, обработки, передачи и защиты информации; – современные программные продукты, необходимые для решения экономико-статистических задач; – методологические подходы к проведению экспериментальных расчетов – теоретические основы оптимизации и исследования операций; – содержательную сторону задач исследования операций, возникающих в экономической практике – сущность и содержание основных категорий и понятий, институтов, правоотношений в отдельных отраслях материального и процессуального права, регулирующих правоотношения в сфере экономики; законодательство Российской Федерации в сфере экономики	Фрагментарное представление об основных методах и средствах поиска, систематизации, обработки, передачи и защиты информации; о современных программных продуктах, необходимых для решения экономико-статистических задач; о методологических подходах к проведению экспериментальных расчетов; о теоретических основах оптимизации и исследования операций; о содержательной стороне задач исследования операций, возникающих в экономической практике; о сущности и содержании основных категорий и понятий, институтов, правоотношений в отдельных отраслях материального и процессуального права, регулирующих правоотношения в сфере экономики; о законодательстве Рос-	Неполные представления об основных методах и средствах поиска, систематизации, обработки, передачи и защиты информации; о современных программных продуктах, необходимых для решения экономико-статистических задач; о методологических подходах к проведению экспериментальных расчетов; о теоретических основах оптимизации и исследования операций; о содержательной стороне задач исследования операций, возникающих в экономической практике; о сущности и содержании основных категорий и понятий, институтов, правоотношений в отдельных отраслях материального и процессуального права, регулирующих правоотношения в сфере экономики; о законодательстве Рос-	Сформированные, но содержащие отдельные пробелы представления об основных методах и средствах поиска, систематизации, обработки, передачи и защиты информации; о современных программных продуктах, необходимых для решения экономико-статистических задач; о методологических подходах к проведению экспериментальных расчетов; о теоретических основах оптимизации и исследования операций; о содержательной стороне задач исследования операций, возникающих в экономической практике; о сущности и содержании основных категорий и понятий, институтов, правоотношений в отдельных отраслях материального и процессуального права, регулирующих правоотношения в	Сформированные систематические представления об основных методах и средствах поиска, систематизации, обработки, передачи и защиты информации; о современных программных продуктах, необходимых для решения экономико-статистических задач; о методологических подходах к проведению экспериментальных расчетов; о теоретических основах оптимизации и исследования операций; о содержательной стороне задач исследования операций, возникающих в экономической практике; о сущности и содержании основных категорий и понятий, институтов, правоотношений в отдельных отраслях материального и процессуального права, регулирующих правоотношения в сфере экономики; о законодательстве Российской Федерации	Реферат, доклад-презентация, тесты, контрольная работа вопросы и задания для проведения зачета

Планируемые результаты освоения компетенции (индикаторы достижения компетенции)	Уровень освоения				Оценочное средство
	неудовлетворительно (минимальный)	удовлетворительно (пороговый)	хорошо (средний)	отлично (высокий)	
	сийской Федерации в сфере экономики	сийской Федерации в сфере экономики	сфере экономики; о законодательстве Российской Федерации в сфере экономики	в сфере экономики	
Уметь: – решать с использованием информационных технологий различные служебные и экономические задачи; – работать в глобальной и локальной компьютерных сетях – использовать модели исследования операций для решения прикладных задач; – использовать информационные системы для решения задач исследования операций – анализировать, толковать и правильно применять правовые нормы, регулирующие отношения в сфере экономики выявлять обстоятельства, способствующие зарождению угроз экономической безопасности и нарушению законодательства	Фрагментарное умение решать с использованием информационных технологий различные служебные и экономические задачи; работать в глобальной и локальной компьютерных сетях; использовать модели исследования операций для решения прикладных задач; использовать информационные системы для решения задач исследования операций; анализировать, толковать и правильно применять правовые нормы, регулирующие отношения в сфере экономики; выявлять обстоятельства, способствующие зарождению угроз экономической безопасности и нарушению законодательства	Несистематическое применение умений решать с использованием информационных технологий различные служебные и экономические задачи; работать в глобальной и локальной компьютерных сетях; использовать модели исследования операций для решения прикладных задач; использовать информационные системы для решения задач исследования операций; анализировать, толковать и правильно применять правовые нормы, регулирующие отношения в сфере экономики; выявлять обстоятельства, способствующие зарождению угроз экономической безопасности и нарушению законодательства	В целом успешное, но содержащее отдельные пробелы умение решать с использованием информационных технологий различные служебные и экономические задачи; работать в глобальной и локальной компьютерных сетях; использовать модели исследования операций для решения прикладных задач; использовать информационные системы для решения задач исследования операций; анализировать, толковать и правильно применять правовые нормы, регулирующие отношения в сфере экономики; выявлять обстоятельства, способствующие зарождению угроз экономической безопасности и нарушению законодательства	Сформированное умение решать с использованием информационных технологий различные служебные и экономические задачи; работать в глобальной и локальной компьютерных сетях; использовать модели исследования операций для решения прикладных задач; использовать информационные системы для решения задач исследования операций; анализировать, толковать и правильно применять правовые нормы, регулирующие отношения в сфере экономики; выявлять обстоятельства, способствующие зарождению угроз экономической безопасности и нарушению законодательства	
Владеть: – методикой построения анализа и применения математических и эконометрических моделей	Отсутствие навыков владения методикой построения анализа и применения математи-	Фрагментарное владение методикой построения анализа и применения математических	В целом успешное, но несистематическое владение методикой построения анализа и при-	Успешное и систематическое владение методикой построения анализа и применения ма-	

Планируемые результаты освоения компетенции (индикаторы достижения компетенции)	Уровень освоения				Оценочное средство
	неудовлетворительно (минимальный)	удовлетворительно (пороговый)	хорошо (средний)	отлично (высокий)	
для оценки состояния и прогнозов развития экономических явлений и процессов; – навыками компьютерной обработки служебной документации, статистической информации и деловой графики; – навыками обеспечения защиты информации, составляющей государственную тайну, и иную служебную информацию – методами математического программирования; навыками работы с нормативными правовыми актами в сфере экономики и экономической безопасности; навыками анализа различных правовых явлений, юридических фактов, правовых норм и правовых отношений, являющихся объектами профессиональной деятельности	ческих и эконометрических моделей для оценки состояния и прогнозов развития экономических явлений и процессов; навыками компьютерной обработки служебной документации, статистической информации и деловой графики; навыками обеспечения защиты информации, составляющей государственную тайну, и иную служебную информацию; методами математического программирования; навыками работы с нормативными правовыми актами в сфере экономики и экономической безопасности; навыками анализа различных правовых явлений, юридических фактов, правовых норм и правовых отношений, являющихся объектами профессиональной деятельности	и эконометрических моделей для оценки состояния и прогнозов развития экономических явлений и процессов; навыками компьютерной обработки служебной документации, статистической информации и деловой графики; навыками обеспечения защиты информации, составляющей государственную тайну, и иную служебную информацию; методами математического программирования; навыками работы с нормативными правовыми актами в сфере экономики и экономической безопасности; навыками анализа различных правовых явлений, юридических фактов, правовых норм и правовых отношений, являющихся объектами профессиональной деятельности	менения математических и эконометрических моделей для оценки состояния и прогнозов развития экономических явлений и процессов; навыками компьютерной обработки служебной документации, статистической информации и деловой графики; навыками обеспечения защиты информации, составляющей государственную тайну, и иную служебную информацию; методами математического программирования; навыками работы с нормативными правовыми актами в сфере экономики и экономической безопасности; навыками анализа различных правовых явлений, юридических фактов, правовых норм и правовых отношений, являющихся объектами профессиональной деятельности	тематических и эконометрических моделей для оценки состояния и прогнозов развития экономических явлений и процессов; навыками компьютерной обработки служебной документации, статистической информации и деловой графики; навыками обеспечения защиты информации, составляющей государственную тайну, и иную служебную информацию; методами математического программирования; навыками работы с нормативными правовыми актами в сфере экономики и экономической безопасности; навыками анализа различных правовых явлений, юридических фактов, правовых норм и правовых отношений, являющихся объектами профессиональной деятельности	
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: – отечественную и международную нормативную базу в соответствующей	Фрагментарное представление об отечественной и международной норма-	Неполные представления об отечественной и международной норма-	Сформированные, но содержащие отдельные пробелы представления	Сформированные систематические представления об отечественной и меж-	Реферат, доклад-презентация, тесты, контрольная

Планируемые результаты освоения компетенции (индикаторы достижения компетенции)	Уровень освоения				Оценочное средство
	неудовлетворительно (минимальный)	удовлетворительно (пороговый)	хорошо (средний)	отлично (высокий)	
области знаний; – научную проблематику соответствующей области знаний; требования к апробации новых алгоритмов.	тивной базе в соответствующей области знаний; о научной проблематике соответствующей области знаний; о требованиях к апробации новых алгоритмов.	тивной базе в соответствующей области знаний; о научной проблематике соответствующей области знаний; о требованиях к апробации новых алгоритмов.	об отечественной и международной нормативной базе в соответствующей области знаний; о научной проблематике соответствующей области знаний; о требованиях к апробации новых алгоритмов.	дународной нормативной базе в соответствующей области знаний; о научной проблематике соответствующей области знаний; о требованиях к апробации новых алгоритмов.	работа вопросы и задания для проведения зачета
Уметь: – применять актуальную нормативную документацию в соответствующей области знаний; – анализировать научную проблематику соответствующей области знаний; разрабатывать рекомендации, методические материалы по направлению деятельности подразделения.	– Фрагментарное умение самостоятельно применять актуальную нормативную документацию в соответствующей области знаний; – анализировать научную проблематику соответствующей области знаний; разрабатывать рекомендации, методические материалы по направлению деятельности подразделения	– Несистематическое применение умений самостоятельно применять актуальную нормативную документацию в соответствующей области знаний; – анализировать научную проблематику соответствующей области знаний; разрабатывать рекомендации, методические материалы по направлению деятельности подразделения	– В целом успешное, но содержащее отдельные пробелы умение самостоятельно применять актуальную нормативную документацию в соответствующей области знаний; – анализировать научную проблематику соответствующей области знаний; разрабатывать рекомендации, методические материалы по направлению деятельности подразделения	Сформированное умение самостоятельно применять актуальную нормативную документацию в соответствующей области знаний; – анализировать научную проблематику соответствующей области знаний; разрабатывать рекомендации, методические материалы по направлению деятельности подразделения	
Владеть: – анализ результатов работ соисполнителей, участвующих в выполнении работ с другими организациями; – разработка ме-	– Отсутствие навыков владения анализом результатов работ соисполнителей, участвующих в выполнении работ с други-	– Фрагментарное владение анализом результатов работ соисполнителей, участвующих в выполнении работ с други-	– В целом успешное, но несистематическое владение анализом результатов работ соисполнителей, участвующих	– Успешное и систематическое владение анализом результатов работ соисполнителей, участвующих в выполнении работ с	

Планируемые результаты освоения компетенции (индикаторы достижения компетенции)	Уровень освоения				Оценочное средство
	неудовлетворительно (минимальный)	удовлетворительно (пороговый)	хорошо (средний)	отлично (высокий)	
роприятий по координации деятельности соисполнителей, участвующих в выполнении работ с другими организациями; апробацией разработанных алгоритмов и приемов отбора информации в целях ПОД/ФТ в организации	ми организациями; – разработкой мероприятий по координации деятельности соисполнителей, участвующих в выполнении работ с другими организациями; апробацией разработанных алгоритмов и приемов отбора информации в целях ПОД/ФТ в организации	ми организациями; – разработкой мероприятий по координации деятельности соисполнителей, участвующих в выполнении работ с другими организациями; апробацией разработанных алгоритмов и приемов отбора информации в целях ПОД/ФТ в организации	в выполнении работ с другими организациями; – разработкой мероприятий по координации деятельности соисполнителей, участвующих в выполнении работ с другими организациями; апробацией разработанных алгоритмов и приемов отбора информации в целях ПОД/ФТ в организации	другими организациями; – разработкой мероприятий по координации деятельности соисполнителей, участвующих в выполнении работ с другими организациями; апробацией разработанных алгоритмов и приемов отбора информации в целях ПОД/ФТ в организации	
ПСК-1 - способностью сбора и обработки информации о финансово- хозяйственной деятельности субъектов хозяйствования различных организационно-правовых форм и отраслевой принадлежности, в том числе в АПК; выявлять взаимосвязь и взаимозависимость экономических и правовых аспектов при раскрытии преступлений в сфере экономики					
Знать: - отечественную и международную нормативную базу в соответствующей области знаний; - основы экономики, организации производства, труда и управления организацией; - методы разработки информационных, объектных, документных моделей производственных организаций	Не обладает знаниями – об отечественной и международной нормативной базе в соответствующей области знаний; – об основах экономики, организации производства, труда и управления организацией; о методах разработки информационных, объектных, документных моделей производственных организаций	Имеет поверхностные знания об отечественной и международной нормативной базе в соответствующей области знаний; – об основах экономики, организации производства, труда и управления организацией; о методах разработки информационных, объектных, документных моделей производственных организаций	Обладает хорошими знаниями об отечественной и международной нормативной базе в соответствующей области знаний; – об основах экономики, организации производства, труда и управления организацией; о методах разработки информационных, объектных, документных моделей производственных организаций	Знает на высоком уровне отечественную и международную нормативную базу в соответствующей области знаний; – основы экономики, организации производства, труда и управления организацией; методы разработки информационных, объектных, документных моделей производственных организаций	Реферат, доклад-презентация, тесты, контрольная работа вопросы и задания для проведения зачета
Уметь: - применять актуальную нормативную документацию в соответствующей обла-	Не умеет применять актуальную нормативную документацию в соответ-	Умеет на низком уровне применять актуальную нормативную	Умеет на достаточном уровне применять актуальную нормативную	Умеет на высоком уровне применять актуальную нормативную документа-	

Планируемые результаты освоения компетенции (индикаторы достижения компетенции)	Уровень освоения				Оценочное средство
	неудовлетворительно (минимальный)	удовлетворительно (пороговый)	хорошо (средний)	отлично (высокий)	
сти знаний; - применять методы разработки информационных, объектных, документных моделей производственных предприятий	ствующей области знаний; применять методы разработки информационных, объектных, документных моделей производственных предприятий	документацию в соответствующей области знаний; применять методы разработки информационных, объектных, документных моделей производственных предприятий	документацию в соответствующей области знаний; применять методы разработки информационных, объектных, документных моделей производственных предприятий	цию в соответствующей области знаний; применять методы разработки информационных, объектных, документных моделей производственных предприятий	
Владеть: - навыками обеспечения научного руководства практической реализацией результатов научных исследований и опытно-конструкторских работ; - навыками контроля реализации внедрения результатов научно-исследовательских и опытно-конструкторских работ; - навыками осуществления подготовки и представления руководству отчета о практической реализации результатов научных исследований и опытно-конструкторских работ	Не владеет навыками обеспечения научного руководства практической реализацией результатов научных исследований и опытно-конструкторских работ; – навыками контроля реализации внедрения результатов научно-исследовательских и опытно-конструкторских работ; навыками осуществления подготовки и представления руководству отчета о практической реализации результатов научных исследований и опытно-конструкторских работ	Слабо владеет навыками обеспечения научного руководства практической реализацией результатов научных исследований и опытно-конструкторских работ; – навыками контроля реализации внедрения результатов научно-исследовательских и опытно-конструкторских работ; навыками осуществления подготовки и представления руководству отчета о практической реализации результатов научных исследований и опытно-конструкторских работ	Хорошо владеет навыками обеспечения научного руководства практической реализацией результатов научных исследований и опытно-конструкторских работ; – навыками контроля реализации внедрения результатов научно-исследовательских и опытно-конструкторских работ; навыками осуществления подготовки и представления руководству отчета о практической реализации результатов научных исследований и опытно-конструкторских работ	Отлично владеет навыками обеспечения научного руководства практической реализацией результатов научных исследований и опытно-конструкторских работ; – навыками контроля реализации внедрения результатов научно-исследовательских и опытно-конструкторских работ; навыками осуществления подготовки и представления руководству отчета о практической реализации результатов научных исследований и опытно-конструкторских работ	

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков, характеризующих этапы формирования компетенций в процессе освоения ОПОП ВО

Темы рефератов (приведены примеры)

1. Деловые ресурсы в Интернет и их защита
2. Компьютерные методы статистического анализа и прогнозирования ИБ
3. Мультимедийные системы обучения и образовательные ИТ, их защита.
4. Развитие представлений об измерении и обработке информации, ее защите.
5. Защита конфиденциальной информации
6. Базовая информационная технология (БИТ) и ее использование в ИБ
7. Специфика проведения отраслевого и регионального анализ. Основные положения теории ИБ для ИС и АИС
8. Разработка модели разграничения доступа к информации. Разграничение доступа к информации
9. Разграничение доступа к информации в среде WindowsXT
10. Требования к системам и средствам ИБ от НСД
11. Контроль за состоянием ИБ.
12. Исследование проблем очистки магнитных носителей
13. Современная ИБ от разрушающих программных воздействий
14. Исследование антивирусных программных средств
15. СЗИ на основе криптографических преобразований
16. Исследование уязвимостей криптографического ПО
17. Базовые принципы обеспечения целостности информации
18. Аппаратные средства опознавания пользователей
19. Принципы функционирования СЗИ от НСД в ПЭВМ
20. Исследование уязвимостей криптографического ПО
21. Исследование программ, защищенных от копирования
22. Специфика работы в среде СЗИ от НСД «SecretNet»
23. Построение системы защиты от НСД для ПК.
24. Тенденции развития защита программ от изучения
25. Новейшие системы ЭЦП

Темы докладов-презентаций(приведены примеры)

1. Модификация автоматизированных обучающих систем (АОС) с учетом требований ИБ.
2. Перспективные направления повышения эффективности ИБ на базе ИТ.
3. Информационные технологии в высшей школе и их защита.
4. Перспективные электронные ИС и ИТ, их защита НСД.
5. Программно-аппаратная защита информации: состояние и перспективы ее развития.
6. Состояние и перспективы развития СЗИ.
7. Модернизация электронных программно-методических комплексов с учетом современных требований к защите авторских прав и информации.

8. Обеспечение ИБ корпоративной ЛВС ФБГОУ ВПО КубГАУ.
9. Перспективные СЗИ для ИПС и БД в экономике.
10. Проблемно-ориентированный информационный консалтинг по ИБ.
11. Автоматизированные обучающие системы и ИБ в них.
12. Современные методы и средства ИБ компьютерной информации.
13. Современные криптографические методы ИБ.
14. Аппаратно-программные средства обеспечения ИБ в компьютерных системах.
15. Методы ИБ в компьютерных системах и сетях.
16. Базовая информационная технология (БИТ) с учетом требований ИБ.
17. Модели разграничения доступа к информации.
18. Развитие представлений об измерении и обработке информации, ее защите.
19. Способы защиты конфиденциальной информации
20. Схема разграничение доступа к информации в среде WindowsXT
21. Иерархия требований к системам и средствам ИБ от НСД
22. Модель типовых криптографических преобразований
23. Схемы уязвимостей криптографической защиты и реализующих ее программ.
24. Связь принципов функционирования СЗИ от НСД в ПК, вычислительных системах и сетях

Вопросы для контрольной работы

1. Объект и предмет защиты. Обоснование функций и задач защиты информации на государственном уровне.
2. Цели и задачи дисциплины "Информационная безопасность". Информационная безопасность (ИБ) в условиях функционирования в России глобальных сетей.
3. Место информационной безопасности экономических и правовых систем в национальной безопасности страны
4. Концепция информационной безопасности. Концептуальная модель ИБ. Основные руководящие нормативные документы, касающиеся государственной тайны и ИБ, нормативно-справочные документы.
5. Основные положения систем защиты информации (СЗИ). Концептуальная модель СЗИ. Основные положения теории ИБ информационных систем.
6. Необходимость защиты информации (ЗИ). Задачи по защите информации в компьютерных системах (КС). Виды возможных нарушений информационной системы. Актуальность проблемы ЗИ. Основные понятия и термины по ЗИ.
7. Модели безопасности и их применение. Классификация методов и средств ЗИ от несанкционированного доступа (НСД). Механизмы защиты информации от НСД. Угрозы конфиденциальной информации.
8. Таксономия нарушений ИБ вычислительной системы и причины, обуславливающие их существование Анализ и оценки угроз конфиденциаль-

ной информации. Возможные виды нарушений ИБ и классификация противников («нарушителей»). Действия, приводящие к неправомерному овладению конфиденциальной информацией.

9. Направления обеспечения ИБ. Государственные требования к построению СЗИ. Концепция ЗИ от НСД. Особые требования к криптографическим средствам СЗИ от НСД. Показатели защищенности СВТ по защите информации от НСД.

10. Классификация АИС и требования по ЗИ. Организационно-правовые аспекты ИБ. Инженерно-техническая защита. Программно-аппаратная защита информации (ПАЗИ).

11. Системы защиты информации (СЗИ) от случайных угроз. Принципы защиты от случайных угроз. Программно-аппаратные методы защиты от случайных угроз. Минимизация ущерба от аварий и стихийных бедствий

12. СЗИ от традиционного шпионажа и диверсий. Система охраны объектов. ЗИ от утечки по техническим каналам. Противодействие НСД к источникам конфиденциальной информации.

13. СЗИ от электромагнитных излучений и закладок. Пассивные методы защиты от побочных электромагнитных излучений и наводок (ПЭМИН). Активные методы защиты от ПЭМИН. Средства выявления и защиты от ПЭМИН

14. ЗИ от несанкционированного изменения структур. Общие требования к защищенности КС от несанкционированного изменения структур. Защита от программных и аппаратных закладок. Защита от несанкционированного изменения структур КС в процессе эксплуатации.

15. Контроль действий пользователей и программ. Задачи контроля в обеспечении безопасности информации. Фиксация доступа к файлам. Способы фиксации факта доступа. Ведение системного журнала. Учет действий программ и пользователей.

16. Регистрация системных событий. Мониторинг функционирования СВТ. Средства контроля администратора безопасности. Средства сигнализации о попытках несанкционированного доступа и выявления нарушителей. Меры противодействия нарушителям.

17. Идентификация и аутентификация субъектов и объектов КС. Идентифицирующая информация. Протоколы идентификации. Основные подходы к защите данных от НСД. Иерархический доступ к файлу. Доступ к данным со стороны процесса.

18. Понятие скрытого доступа. Модели управления доступом. Дискреционная (избирательная) и мандатная (полномочная) модели управления доступом. ЗИ от несанкционированного доступа (НСД). Система разграничения доступа к информации в компьютерных системах (КС). Требования к системам и средствам ЗИ от НСД. Защита программных средств от копирования и исследования.

19. Понятие разрушающего программного воздействия (РПВ). Сущность разрушающих программных средств. Взаимодействие прикладных программ и программы-злоумышленника. Классификация разрушающих

программных средств и их воздействий. Компьютерные вирусы (КВ) как особый класс РПВ. Сущность, проявление, классификация компьютерных вирусов. Компьютерные вирусы (КВ).

20. Механизмы борьбы с КВ. Методы и средства борьбы с компьютерными вирусами. Профилактика заражения КВ и действия пользователя при заражении ЭВМ вирусами. Принципы и методы защиты от РПВ. Анализ программного обеспечения с целью выявления разрушающих программных компонентов.

21. Требования ГТК к ПО СЗИ и его классификация по уровню контроля отсутствия не декларированных возможностей. Необходимые и достаточные условия недопущения разрушающего воздействия: понятие изолированной программной среды. Организационные средства защиты от компьютерных вирусов. Роль морально-этических факторов в устранении угрозы РПВ.

22. Принципы криптографической ЗИ и ее применение в КС. Классификация методов криптографического преобразования информации. Методы и стандарты шифрования. Перспективы использования криптозащиты информации в компьютерных системах. Защита алгоритма шифрования. Программно-аппаратные средства шифрования.

23. Принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты. Построение аппаратных компонент криптозащиты данных. Краткая характеристика систем криптографической защиты данных на основе плат "КРИПТОН".

24. Криптографические средства обеспечения целостности информации. Проблема и способы обеспечения целостности информации. Защита файлов от изменений. Электронная цифровая подпись (ЭЦП).

25. Криптографические хэш-функции. Схемы вычисления хэш-функции. Методы криптографии. Задачи, решаемые криптографическими средствами в КС. Алгоритмы криптографических преобразований и их характеристики.

26. ЗИ в распределенных компьютерных системах (КС). Международные стандарты информационного обмена. Архитектуры распределенных компьютерных систем и особенности ЗИ в них. ИБ в условиях функционирования в России глобальных вычислительных систем

27. Теория создания компьютерных систем защиты информации (СЗИ). Концепция создания защищенных компьютерных систем. Использование защищенных компьютерных систем. Основные технологии построения защищенных экономических и правовых ИС. Методология проектирования компьютерных СЗИ. Моделирование компьютерных СЗИ и их оценка.

28. Проектирование компьютерных СЗИ. Выбор показателей эффективности и критерия оптимальности компьютерной СЗИ. Этапы создания комплексной СЗИ. Создание организационной структуры компьютерной СЗИ.

29. Организация функционирования компьютерных СЗИ. Применение компьютерных СЗИ в экономике и в юриспруденции. Техническая эксплуатация компьютерных СЗИ. Построение системы защиты от НСД для ПЭВМ. Методы и средства ограничения доступа к компонентам ЭВМ. Надежность систем ограничения доступа.

30. Построение средств защиты информации для ПЭВМ. Перечень и краткая характеристика сертифицированных программных и программно-аппаратных средств СЗИ от НСД для ПЭВМ. Особенности защиты информации в вычислительных сетях. Механизмы реализации атак на вычислительные сети. Защита сетевого файлового ресурса.

Тесты (приведены примеры):

1. Рекомендации ФСТЭК России по формированию экспертной группы (ЭГ)

а) федеральными стандартами

б) отраслевыми стандартами

в) рекомендациями в области бухгалтерского учета

г) стандартами экономического субъекта

2. Перечень всех специалистов, из которых формируется экспертная группа на предприятии.

а) обладателей информации

б) разработчиков АСУ и операторов АИС

в) специалистов по защите информации (ЗИ)

г) операторов, взаимодействующих с внешними информационными системами

3. Количество членов ЭГ на предприятии:

а) ≥ 3

б) 4

в) 5

г) 7

4. Расчет денежных средств, необходимых для обеспечение нужной ИБ на конкретном предприятии:

а) анализ денежных затрат на ИБ с учетом действующего законодательства, стоимости оборудования по ЗИ и фактического экономического состояния организации;

б) анализ организационной структуры экономического субъекта, состава его информации, необходимой заинтересованным пользователям;

в) постановка цели формирования политики ИБ, разработка ее структуры и этапов реализации;

г) определение аспектов политики ИБ, ее составляющих элементов, разработка документации, раскрывающей их особенности.

5. Технология оценки потенциала нарушителя, необходимого для реализации угроз безопасности информации:

а) < 10 потенциал недостаточен

б) 10-17 базовый (низкий)

в) 18-24 базовый повышенный (средний)

г) >24 высокий

6. Описание ИС и особенностей ее функционирования:

а) цель и задачи, решаемые ИС

б) структурно-функциональных характеристик ИС

в) технологий обработки информации

г) >24 высокий

7. Описание возможностей нарушений ИБ экономического предприятия:

а) < 10 потенциал недостаточен

б) 10-17 базовый (низкий)

в) 18-24 базовый повышенный (средний)

г) >24 высокий

8. Технология бальной оценки невозможности реального доступа нарушителя к ИС:

а) < 0,5 часа

б) 1 день

в) > 1 месяца

г) не возможен

9. Курс информационной безопасности связан с:

а) математической логикой

б) кибернетикой

в) информатикой

г) правовыми науками

д) математическими науками

10. Подготовка данных к машинной (компьютерной) обработке это:

а) перекодировка информации любой природы в данные, используемые компьютером при его работе

б) преобразование входной информации

в) ввод информации в ЭВМ с помощью устройств преобразования информации

г) считывание информации с машинных носителей

д) преобразование выходной информации

Вопросы и задания для проведения промежуточного контроля

Компетенция: способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12);

Вопросы к зачету

1. Структура и функции подсистемы контроля доступа программ и пользователей.

2. Средства активного аудита компьютерных систем.

3. Идентификация и аутентификация субъектов и объектов КС.
4. Идентифицирующая информация и протоколы идентификации.
5. Основные подходы к защите данных от НСД.
6. Иерархический доступ к файлу.
7. Доступ к данным со стороны процесса.
8. Понятие скрытого доступа.
9. Модели управления доступом.
10. Особые требования к криптографическим средствам СЗИ от НСД.
11. Показатели защищенности СВТ от НСД.
12. Классификация КС и требования по защите информации.
13. Использование защищенных компьютерных систем.
14. Работа пользователей ПК в защищенной среде.
15. Методы контроля доступа к ресурсам компьютерной системы.
16. Способы фиксации факта доступа.
17. Средства контроля вычислительных процессов.
18. Свойства процессов и управление ими.
19. Средства гарантированного удаления информации.
20. Средства анализа программ.

Задания для проведения зачета (приведены примеры)

1. Определить уязвимость КС и выбрать средства защиты информации.
2. Создать учетные записи пользователей.
3. Создать учетные записи групп.
4. Организация общего доступа к папкам.
5. Анализ системных журналов ОС Windows NT и средства ведения
6. Восстановить удаленные файлы
7. Восстановить отформатированные диски.
8. Дизассемблирование программ и исследование кода.
9. Исследование дискет, защищенных от копирования
10. Исследование программ с защитой от копирования.

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

Вопросы к зачету

1. Международные стандарты информационного обмена.
2. Концепция информационной безопасности.
3. Место информационной безопасности экономических систем в национальной безопасности страны.
4. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

5. Таксономия нарушений информационной безопасности вычислительной системы

6. Три вида возможных нарушений информационной системы

7. Актуальность проблемы защиты информации.

8. Модели безопасности и их применение.

9. Классификация методов защиты информации от НСД.

10. Классификация средств защиты информации от НСД.

11. Механизмы защиты информации от НСД.

12. Государственные требования к построению СЗИ.

13. Концепция защиты информации от НСД.

14. Дискреционная (избирательная) и мандатная (полномочная) модель управления доступом.

15. Защита алгоритма шифрования и программно-аппаратные средства шифрования.

Задания для проведения зачета (приведены примеры)

1. Защита программ от отладки.
2. Защита программ от трассировки.
3. Антивирусные программные комплексы. Настройка и применение.
4. Активный контроль состояния безопасности компьютерной системы.
5. Устранение проникновения вирусов в компьютерную систему.
6. Исследование результатов воздействия компьютерных вирусов на программы в среде ОС
7. Исследование результатов работы антивирусных программ.
8. Защита файлов и каталогов. Шифрованные логические диски.
9. Средства анализа и копирования защищенных дискет и взламывания защиты программ.
10. Средства простановки ключевых меток и защиты программ от копирования.

Компетенция: способностью сбора и обработки информации о финансово- хозяйственной деятельности субъектов хозяйствования различных организационно-правовых форм и отраслевой принадлежности, в том числе в АПК; выявлять взаимосвязь и взаимозависимость экономических и правовых аспектов при раскрытии преступлений в сфере экономики (ПСК-1).

Вопросы к зачету

1. Построение аппаратных компонент криптозащиты данных.
2. Сущность разрушающих программных средств.
3. Взаимодействие прикладных программ и программы-злоумышленника.
4. Классификация разрушающих программных средств и их воздействий.
5. Компьютерные вирусы как особый класс РПВ.
6. Сущность, проявление, классификация компьютерных вирусов.

7. Необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды.

8. Организационные средства защиты от компьютерных вирусов.

9. Роль морально-этических факторов в устранении угрозы РПВ.

10. Проблема обеспечение целостности информации.

11. Защита файлов от изменений. Способы обеспечения целостности информации.

12. Электронная цифровая подпись. Криптографические хэш-функции. Схемы вычисления хэш-функции.

13. Методы криптографии и задачи, решаемые криптографическими средствами в КС.

14. Алгоритмы криптографических преобразований и их характеристики.

15. Методы и средства ограничения доступа к компонентам ЭВМ.

16. Построение средств защиты информации для ПЭВМ.

17. Перечень и краткая характеристика сертифицированных программно-аппаратных систем защиты информации (СЗИ) от НСД для ПЭВМ.

18. Особенности защиты информации в вычислительных сетях.

19. Механизмы реализации атак на вычислительные сети.

20. Защита сетевого файлового ресурса.

21. Определение перечня защищаемых ресурсов и их критичности.

22. Определение категорий персонала и программно-аппаратных средств, на которые распространяется политика безопасности.

23. Определение угроз безопасности информации.

24. Формирование требований к построению СЗИ.

25. Централизованное управление пользователями и контроль их действий.

Задания для проведения зачета (приведены примеры):

1. Алгоритмы ЭЦП. Реализация ЭЦП В СКЗИ «Верба-OW».
2. Построение СЗИ "Кобра".
3. Администрирование СЗИ "Кобра".
4. Исследование временной стойкости криптосистемы архиватора WinZip.
5. Исследование уязвимостей криптосистемы архиватора Arj.
6. Построение аппаратных средств СЗИ "Аккорд" и управление пользователями в ней.
7. Построение и принцип работы программ СЗИ "Снег-1.0", работа ее администратора.
8. Работа администратора при использовании СЗИ от НСД "SecretNet".
9. Работа администратора ЛВС по управлению пользователями.
10. Работа администратора ЛВС по управлению доступом пользователей и процессов к ресурсам системы.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков характеризующих этапы формирования компетенций

Контроль освоения дисциплины и оценка знаний обучающихся производится в соответствии с Пл. КубГАУ 2.5.1 «Текущий контроль и успеваемости и промежуточной аттестации обучающихся».

Критериями оценки доклада, реферата являются: качество текста, обоснованность выбора источников литературы, степень раскрытия сущности вопроса, соблюдения требований к оформлению и представлению результатов.

Оценка «**отлично**» – выполнены все требования к написанию реферата, представлению доклада обозначена проблема и обоснована её актуальность; сделан анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция; сформулированы выводы, тема раскрыта полностью, выдержан объём; соблюдены требования к внешнему оформлению.

Оценка «**хорошо**» – основные требования к реферату, докладу выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата. доклада; имеются нарушения в оформлении.

Оценка «**удовлетворительно**» – имеются существенные отступления от требований к реферированию и представлению доклада. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата, доклада; отсутствуют выводы.

Оценка «**неудовлетворительно**» – тема реферата, доклада не раскрыта, обнаруживается существенное непонимание проблемы или реферат, доклад не представлен вовсе.

Оценочный лист реферата (доклада)

ФИО обучающегося _____

Группа_____ преподаватель _____

Дата_____

Наименование показателя	Выявленные недостатки и замечания	Оценка
Качество		
1. Соответствие содержания заданию		
2. Грамотность изложения и качество оформления		
3. Самостоятельность выполнения,		
4. Глубина проработки материала,		
5. Использование рекомендованной и справочной литературы		
6. Обоснованность и доказательность выводов		
Общая оценка качества выполнения		
Защита реферата (Представление доклада)		
1. Свободное владение профессиональной терминологией		

2. Способность формулирования цели и основных результатов при публичном представлении результатов		
3. Качество изложения материала (презентации)		
Общая оценка за защиту реферата		
Ответы на дополнительные вопросы		
Вопрос 1.		
Вопрос 2.		
Вопрос 3.		
Общая оценка за ответы на вопросы		
Итоговая оценка		

Критерии оценки знаний при написании контрольной работы

Оценка «**отлично**» – выставляется обучающемуся, показавшему всесторонние, систематизированные, глубокие знания вопросов контрольной работы и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка «**хорошо**» – выставляется обучающемуся, 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, которые может устранить с помощью дополнительных вопросов преподавателя.

Оценка «**удовлетворительно**» – выставляется обучающемуся, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными понятиями выносимых на контрольную работу тем, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка «**неудовлетворительно**» – выставляется обучающемуся, который не знает большей части основного содержания выносимых на контрольную работу вопросов тем дисциплины, допускает грубые ошибки в формулировках основных понятий и не умеет использовать полученные знания при решении типовых практических задач.

Критерии оценки знаний при проведении тестирования

Оценка «**отлично**» выставляется при условии правильного ответа студента не менее чем на 85 % тестовых заданий;

Оценка «**хорошо**» выставляется при условии правильного ответа студента не менее чем на 70 % тестовых заданий;

Оценка «**удовлетворительно**» выставляется при условии правильного ответа студента не менее чем на 51 %;

Оценка «**неудовлетворительно**» выставляется при условии правильного ответа студента менее чем на 50 % тестовых заданий.

Результаты текущего контроля используются при проведении промежуточной аттестации.

Критерии оценки знаний обучающихся при проведениизачета

Оценка **«зачтено»** – дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи. Могут быть допущены недочеты в определении понятий, исправленные обучающимся самостоятельно в процессе ответа.

Оценка **«не зачтено»** – допущены грубые ошибки при определении сущности раскрываемых понятий, теорий, явлений, вследствие непонимания обучающихся их существенных и несущественных признаков и связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано.

8 Перечень основной и дополнительной учебной литературы

Основная учебная литература

1. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — Режим доступа: http://www.iprbookshop.ru/86938.html

2. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е.В. Глинская, Н.В. Чичварин. — Москва : ИНФРА-М, 2021. — 118 с. + Доп. материалы [Электронный ресурс]. — DOI 10.12737/13571. - ISBN 978-5-16-010961-9. - Режим доступа: https://znanium.com/catalog/product/1178152

3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2019. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Режим доступа: https://znanium.com/catalog/product/1009605

Дополнительная учебная литература

1. Информационные ресурсы и технологии в экономике : учеб. пособие / под ред. проф. Б.Е. Одинцова и проф. А.Н. Романова. — М. : Вузовский учебник: ИНФРА-М, 2019. — 462 с. - Текст : электронный. – Режим доступа: https://new.znanium.com/catalog/product/1032991

2. Анисимов, А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 211 c. — ISBN 978-5-4497-0328-6. — Режим доступа: http://www.iprbookshop.ru/89443.html

3. Одинцов, Б. Е. Современные информационные технологии в управлении экономической деятельностью (теория и практика) : учебное пособие / Б.Е. Одинцов, А.Н. Романов, С.М. Догучаева. — Москва : Вузовский

учебник : ИНФРА-М, 2020. — 373 с. - ISBN 978-5-16-102337-2. - Текст : электронный. – Режим доступа: https://new.znanium.com/catalog/product/1047195

4. Петров, С. В. Информационная безопасность [Электронный ресурс] : учебное пособие / С. В. Петров, П. А. Кисляков. — Электрон. текстовые данные. — Саратов : Ай Пи Ар Букс, 2015. — 326 с. — 978-5-906-17271-6. — Режим доступа: http://www.iprbookshop.ru/33857.html

5. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2020. — 336 с. — (Высшее образование). - ISBN 978-5-369-01761-6. - Режим доступа: https://znanium.com/catalog/product/1114032

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронно-библиотечных систем

№	Наименование	Тематика	Ссылка
1.	Znanium.com	Универсальная	https://znanium.com/
2.	IPRbook	Универсальная	http://www.iprbookshop.ru/
3.	Образовательный портал КубГАУ	Универсальная	https://edu.kubsau.ru/

Перечень рекомендуемых интернет сайтов:

1. Правила информационной безопасности в интернете [Электронный ресурс]. – Электрон. дан. – URL: https://mensby.com/career/psychology/pravila-informacionnoj-bezopasnosti-v-internete

2. Опасности социальных сетей [Электронный ресурс]. – Электрон. дан. – URL: http://www.wsms.ru/news/programmirovanie/opasnosti_setey.shtml

10 Методические указания для обучающихся по освоению дисциплины

1. Информационная безопасность: метод. рекомендации по организации самостоятельной работы студентов, обучающихся по специальности 38.05.01 Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности»/ сост.: В. Н. Лаптев. – Краснодар: КубГАУ, 2020. – 31 с. Режим доступа: https://edu.kubsau.ru/file.php/118/_38.05.01_EHB_IB_MU_po_org_SR_Laptev_Melnikov_Snimshchikova_2020_570174_v1_.PDF

2.Информационная безопасность: Практикум для студентов. – /В. И. Лойко., В. Н. Лаптев. – Краснодар: КубГАУ, – 128с. (в электронном виде на кафедре КТС).

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

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине позволяют: обеспечить взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети "Интернет"; фиксировать ход образовательного процесса, результатов промежуточной аттестации по дисциплине и результатов освоения образовательной программы; организовать процесс образования путем визуализации изучаемой информации посредством использования презентационных технологий; контролировать результаты обучения на основе компьютерного тестирования.

Перечень лицензионного ПО

№	Наименование	Краткое описание
1	Microsoft Windows	Операционная система
2	Microsoft Office (включает Word, Excel, PowerPoint)	Пакет офисных приложений
3	Система тестирования INDIGO	Тестирование

Перечень профессиональных баз данных и информационных справочных систем

№	Наименование	Тематика	Электронный адрес
1	Научная электронная библиотека eLibrary	Универсальная	https://elibrary.ru/
2	Гарант	Правовая	https://www.garant.ru/
3	КонсультантПлюс	Правовая	https://www.consultant.ru/

12 Материально-техническое обеспечение для обучения по дисциплине

Планируемые помещения для проведения всех видов учебной деятельности

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)

1	Информационная безопасность	Помещение №312 ЭК, посадочных мест — 167; площадь — 165,4 кв.м.; учебная аудитория для проведения занятий лекционного типа. специализированная мебель(учебная доска, учебная мебель); технические средства обучения, наборы демонстрационного оборудования и учебно-наглядных пособий (ноутбук, проектор, экран); программное обеспечение: Windows, Office. Помещение №1 ЭК, площадь — 64,9 кв.м.; посадочных мест — 30; учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации кондиционер — 1 шт.; технические средства обучения (компьютер персональный — 15 шт.); доступ к сети «Интернет»; доступ в электронную информационно-образовательную среду университета; специализированная мебель(учебная доска, учебная мебель). Помещение №3 ЭК, посадочных мест — 30; площадь — 62,1 кв.м.; учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. сплит-система — 1 шт.; кондиционер — 1 шт.; технические средства обучения (сетевое оборудование — 1 шт.; компьютер персональный — 16 шт.); доступ к сети «Интернет»; доступ в электронную информационно-образовательную среду университета; специализированная мебель (учебная доска, учебная мебель). программное обеспечение: Windows, Office, INDIGO. Помещение №4 ЭК, площадь — 31,1 кв.м.; помещение для хранения и профилактического обслуживания учебного оборудования. кондиционер — 2 шт.; лабораторное оборудование (шкаф лабораторный — 1 шт.; набор лабораторный — 1 шт.;); технические средства обучения (принтер — 1 шт.; проектор — 1 шт.; микрофон — 1 шт.; ибп — 4 шт.; сервер — 1 шт.; носитель информации — 1 шт.; компьютер персональный — 15 шт.). Помещение №211а НОТ, посадочных мест — 30; площадь — 47,1 кв.м.; помещение для самостоятельной работы. технические средства обучения (принтер — 2 шт.; экран — 1 шт.; проектор — 1 шт.; сетевое оборудование — 1 шт.; ибп — 1 шт.; компьютер персональный — 6 шт.);	350044, Краснодарский край, г. Краснодар, ул. им. Калинина, 13

		доступ к сети «Интернет»; доступ в электронную информационно-образовательную среду университета; специализированная мебель (учебная мебель). Программное обеспечение: Windows, Office, специализированное лицензионное и свободно распространяемое программное обеспечение, предусмотренное в рабочей программе	