Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кубанский государственный университет»
Экономический факультет

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Хагуров Т.А.
подпись
«___» _____ 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.06 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование дисциплины в соответствии с учебным планом)

Направление подготовки 38.03.05 Бизнес-информатика
(код и наименование направления подготовки)

Направленность (профиль) Электронный бизнес
(наименование направленности (профиля))

Программа подготовки Академическая
(академическая /прикладная)

Форма обучения Очная
(очная, очно-заочная, заочная)

Квалификация (степень) выпускника Бакалавр
(бакалавр, магистр)

Краснодар 2019

1. Цели и задачи изучения дисциплины

1.1. Цели и задачи дисциплины

Цель дисциплины: заложить методически правильные основы знаний, необходимые будущим специалистам-практикам в области информационной безопасности; формирование у студентов бакалавриата представления об особенностях режима информационной безопасности в структурных подразделениях высокотехнологичных фирм. Курс должен дать представление об объективных возможностях и фактических результатах использования возможностей высокотехнологичного компьютерного обеспечения информационной безопасности; показать общее и специфическое в механизмах, инфраструктуре, информационном обеспечении необходимого уровня конфиденциальности в функционировании фирмы; раскрыть специфические особенности опасностей использования элементов облачных технологий в деятельности фирмы.

Задачи дисциплины:

1.Раскрытие содержания понятия «информационная безопасность».

2. Усвоение современного, согласованного с другими ветвями ИТ категориального базиса.

3. Описание общей структуры и отдельных уровней комплексного подхода в области информационной безопасности(ИБ).

4.Изучение механизма взаимодействия сотрудников высокотехнологичного/электронного предприятия.

5.Рассмотрение организационно-правовых форм обеспечения информационной безопасности высокотехнологичного/электронного бизнеса.

6.Изучение специфики обеспечения информационной безопасности в области промышленной собственности и хозяйственной деятельности высокотехнологичного/электронного предприятия.

1.2. Место дисциплины в структуре образовательной программы:

Дисциплина имеет шифр Б1.В.06 учебного плана подготовки бакалавров направления 38.03.05 Бизнес-информатика, профиль подготовки «Электронный бизнес» - Вариативная часть. Логически дисциплина увязана с такими основными базовыми курсами как «Теоретические основы информатики», «Менеджмент» и является дальнейшим развитием прикладных аспектов названных дисциплин.

Для освоения дисциплины студент должен обладать:

1. базовыми входными знаниями в области:

- общей экономической теории;
- микроэкономики;
- макроэкономики;

2. умениями в области:

- осуществления поиска информации;
- обработки данных с использованием соответствующих компьютерных программ;
- логической увязки картины событий в условиях неполной информации;
- строить адекватные ситуации выводы, заключения на основе анализа имеющихся данных.

1.3.Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих профессиональных компетенций: ПК-9; ПК-11.

№№ п/п	Индекс компетенции	Содержание компетенции(или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-9	Организация взаимодействия с клиентами и партнёрами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия.	основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках	видеть и формулировать проблему; видеть конкретную ситуацию; прогнозировать и предвидеть; ставить цели и задачи	навыками самостоятельного усвоения новых знаний в области обеспечения информационной безопасности высокотехнологичного/ электронного предприятия
	ПК-11	Умение защищать права на интеллектуальную собственность	законодательство, корресподирующееся с дефинициями «интеллектуальная собственность/нематериальные активы	Выявить уязвимости с целью упреждения негативных тенденций и процессов	пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа.

2.Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 3 зач. ед. (108 часов), их распределение по видам работ представлено в таблице*(для студентов ОФО)*.

Вид учебной работы	Всего часов	Семестры(часы)			
		4	5	6	7
Контактная работа, в том числе					
Аудиторные занятия (всего)	**52**	**-**	**52**	**–**	**–**
Занятия лекционного типа	18	-	18	–	–
Лабораторные занятия	-	-	-	–	–
Занятия семинарского типа (семинары, практические занятия)	34	-	34	–	–
Иная контактная работа	**2,3**	**-**	**2,3**	**–**	**–**
Контроль самостоятельной работы (КСР)	2	-	2	–	–
Промежуточная аттестация (ИКР)	0,3	-	0,3	–	–
Самостоятельная работа (всего)	**27**	**-**	**27**	**–**	**–**
В том числе:					
Проработка учебного(теоретического) материала	10	-	10	–	–
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)	10	-	10	–	–

Курсовая работа		-		-	–	–
Вид промежуточной аттестации		экза-мен		экза-мен		
Подготовка к текущему контролю		7	-	7	–	–
Контроль						
Подготовка к экзамену		26,7	-	26,7	–	–
Общая трудоёмкость	**Час**	**108**	**-**	**108**	**-**	**-**
	в том числе контактная работа	**54,3**	**-**	**54,3**	**-**	**-**
	зач. ед. (ЗЕ)	**3**	**-**	**3**	**-**	**-**

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоёмкости по разделам дисциплины. Разделы(темы) дисциплины, изучаемые в 5 семестре

№	Наименование раздела	Количество часов				
		Всего	Аудиторная работа			СР
			Л	ПЗ	ЛР	
1.	Введение. Предмет и задачи информационной безопасности	8	2	2	-	4
2.	Концепция безопасности в компьютерной архитектуре	8	2	2	-	4
3.	Архитектура информационной безопасности	12	2	6	-	4
4.	Контроль доступа	13	4	6	-	3
5.	Модели контроля доступа	12	2	6	-	4
6.	Угрозы и уязвимости	14	4	6	-	4
7.	Основы криптографической защиты информации	12	2	6	-	4
	Итого		**18**	**34**	**-**	**27**

Примечание: Л – лекции, ПЗ – практические занятия/семинары, ЛР – лабораторные занятия, СР –самостоятельная работа студента.

2.3.Содержание разделов (тем) дисциплины

2.3.1.Занятия лекционного типа

№ раздела	Наименование раздела (темы)	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Введение. Предмет и задачи академической дисциплины «Информационная безопасность».	Национальная безопасность в современных условиях. Роль и место безопасности в жизнедеятельности человека и общества. Общеметодологические принципы обеспечения информационной безопасности. Предмет информационной безопасности.	Р, контрольные вопросы
2.	Информационная сфера как область противо-	1. Общие основы теории информационного противоборства	Р, контрольные вопросы

	борства в XXI в.	2. Информационная война. Информационные операции	Р Р, контрольные вопросы
		3. Информационное оружие - общие положения	Р
3.	Информационная безопасность информационных систем(ИБ ИС).	1. Виды и классификация угроз информационным системам	Р
		2. Методы и средства обеспечения информационной безопасности.	Р, контрольные вопросы
		3. Угрозы конфиденциальности, целостности и доступности	Э, Р, контрольные вопросы
4.	Общие проблемы безопасности. Роль и место информационной безопасности.	1. Национальные интересы и безопасность России.	Р, контрольные вопросы
		2.Информационное превосходство в обычных и информационных войнах.	Р, контрольные вопросы
		3.Принципы, основные задачи и функции обеспечения информационной безопасности.	Р
		4.Функции государственной системы по обеспечению информационной безопасности	Р, контрольные вопросы
5.	Защита информации в автоматизированных системах	1.Предмет и объекты защиты информации в автоматизированных системах обработки данных (АСОД).	Р, контрольные вопросы
		2.Причины нарушения целостности информации (ПНЦИ). Каналы несанкционированного получения информации в АСОД (КНПИ).	Р, контрольные вопросы
		3.Функции и задачи защиты информации. Методы и системы защиты информации.	Р, контрольные вопросы
6.	Криптографические методы защиты информации	1.Функции, выполняемые криптологическим протоколом.	Э
		2.Электронная цифровая подпись как гарантированное подтверждение подлинности информации, содержащейся в конкретном электронном документе	Р
		3.Криптографические стандарты DES и ГОСТ 28147—89. Проблемы реализации методов криптографической защиты в АСОД.	Р Р, контрольные вопросы
7.	Защита информации в персональных компьютерах	1.Особенности защиты информации в персональных ЭВМ	Р
		2.Защита ПК от несанкционированного доступа. Физическая защита ПК и носителей информации	Р
		3.Защита ПК от вредоносных закладок (разрушающих программных средств). Классификация закладок и их общие характеристики	Р, контрольные вопросы
8	Компьютерные вирусы и антивирусные программы	1.Угрозы и уязвимости безопасности информации в ИС.	Р, контрольные вопросы
		2.Защита программ от несанкционированного копирования	Р, контрольные вопросы
		3.Антивирусная программа DRWEB. Kaspersky Anti-Virus 2016.	Р, контрольные вопросы
9	Проблемы защиты ин-	1.Цели, функции и задачи защиты информации в	Р, контрольные

	формации в сетях ЭВМ.	сетях ЭВМ.	вопросы
		2.Архитектура механизмов защиты информации в сетях ЭВМ	Р, контрольные вопросы
		3.Межсетевые экраны — брандмауэры (FireWall).Прокси (Proxy) серверы	Р, контрольные вопросы
10	Технические средства и комплексное обеспечение безопасности	1.Комплексный подход к обеспечению безопасности	Р, контрольные вопросы
		2.Биометрические системы идентификации	Р, контрольные вопросы
		3.Охранные системы МИККОМ	Р, Э

2.3.2 Практические занятия

№	Наименование раздела (тем)	Тематика практических занятий (семинаров)	Форма текущего контроля
1	2	3	4
1.	Информационная безопасность: введение в курс	Цели, актуальность и общее содержание курса обучения. Актуальность проблемы защиты информации. Основные понятия, термины и определения. Категории информации	Р, тест
2.	Правовые основы обеспечения защиты информации.	Государственная система защиты информации. Нормативные акты правового регулирования вопросов информатизации и защиты информации в России. Структура, задачи и основные функции Государственной системы защиты информации. Лицензирование. Сертификация средств защиты. Аттестация объектов информатизации.	Р, тест
3.	Технические каналы утечки информации	Классификация технических каналов утечки информации. Каналы утечки речевой информации. Примеры, механизмы реализации.Утечка речевой информации по проводам ПЭМИН. Примеры, механизмы реализации. Выявление технических каналов утечки информации. Методы и средства выявления каналов утечки информации. Классификация аппаратуры выявления каналов утечки. Принципы функционирования и особенности эксплуатации аппаратуры. Демонстрация возможностей. Рекомендации по выбору и применению.	Р, тест
4.	Основы информационной безопасности объектов обработки информации	Информация как объект защиты. Автоматизированные системы обработки информации как объекты защиты. Структура АС, характеристики средств автоматизации, характеристики информационных ресурсов АС, категории защищаемой информации, классификация АС.	Р, тест

		Угрозы безопасности конфиденциальной информации, цели и способы реализации угроз.	
5.	Основы организации и обеспечения работ по технической защите информации	Цели, задачи защиты информации, способы и средства их реализации. Классификация способов и средств защиты информации. Основные механизмы защиты информации. Структура и принципы построения системы технической защиты информации предприятия. Организация подразделений (служб) обеспечения информационной безопасности, их функции и задачи. Определение перечня сведений конфиденциального характера, подлежащих защите. Оценка опасности угроз при применении современных информационных технологий. Разработка концепции (политики) информационной безопасности предприятия. Планирование работ по защите информации. Обоснование требований к системе защиты информации. Классификация объектов информатизации по требованиям безопасности информации. Проектирование, создание и эксплуатация системы защиты информации. Основные требования и реализация руководящих документов по технической защите конфиденциальной информации.	Р, тест
6.	Типовые средства защиты информации и особенности их эксплуатации. Основные методы и средства защиты информации от утечки по техническим каналам. Требования к применяемым средствам защиты информации	Классификация средств защиты информации по видам объектов обрабатывающих конфиденциальную информацию (каналы связи, помещения для ведения конфиденциальных переговоров, автоматизированные системы и т.д.). Средства защиты информации от утечки по техническим каналам. Характеристики средств защиты, назначение, реализуемые функции, состав. Системы виброакустического зашумления. Назначение, обзор моделей, технические характеристики, особенности применения. Рекомендации по установке (настройке) и эксплуатации. Рекомендации по выбору. Средства защиты от утечки по ПЭМИН. Назначение, обзор моделей, технические характеристики, особенности применения. Рекомендации по установке (настройке) и эксплуатации. Рекомендации по выбору. Средства защиты слаботочных линий. Назна-	Р, тест

		чение, обзор моделей, технические характеристики, особенности применения. Рекомендации по установке (настройке) и эксплуатации. Рекомендации по выбору. Средства защиты сети питания. Назначение, обзор моделей, технические характеристики, особенности применения. Устройства защиты телефонных линий. Назначение, обзор моделей, технические характеристики, особенности применения. Рекомендации по установке (настройке) и эксплуатации. Рекомендации по выбору. Средства защиты автоматизированных систем. Штатные средства защиты операционных систем (на примере Windows, Unix и др.). Настройка операционных систем, характеристика уязвимых мест ОС. Штатные средства защиты СУБД. Обзор возможностей. Средства защиты информации от НСД. Рекомендации по выбору. Межсетевые экраны - как средства защиты информации при межсетевом взаимодействии. Их характеристика. Демонстрация возможностей. Механизмы для создания виртуальных частных сетей (VPN). Методы организации VPN. Основные возможности и характеристики. Обзор отечественных и зарубежных антивирусных продуктов. Основные характеристики и механизмы функционирования. Особенности применения различных антивирусных средств. Рекомендации по выбору антивирусных продуктов.	
7.	Средства контроля защищённости автоматизированных систем	Методы контроля защищённости автоматизированной системы. Обзор средств контроля. Инструментальные средства для проведения контроля эффективности настройки систем защиты от НСД автоматизированной системы. Примеры функционирования, принципы и особенности работы. Сканеры безопасности. Их назначение. Принципы работы. Примеры сканеров. Средства обнаружения атак. Их назначение. Принципы работы. Примеры средств обнаружения атак.	Р, тест
8.	Средства оценки защищённости информации по техническим каналам	Методы оценки защищённости информации от утечки по техническим каналам. Обзор средств контроля защищённости. Аппаратура контроля защищённости помеще-	Р, тест

		ния по акустическим и виброакустическим каналам. Аппаратура контроля защищённости автоматизированных систем от утечки по каналам ПЭМИН.	

2.3.3 Лабораторные занятия

Лабораторные занятия не предусмотрены учебным планом.

2.3.4 Примерная тематика курсовых работ

Курсовые работы не предусмотрены учебным планом.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СР	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Проработка и повторение лекционного материала, материала учебной и научной литературы, подготовка к практическим занятиям, подготовка рефератов (презентаций).	Методические указания для подготовки эссе, рефератов, курсовых работ (Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 8 от 29 июня 2017 г.) http://docspace.kubsu.ru/docspace/handle/1/1120 Методические указания для подготовки к занятиям лекционного и семинарского типа (Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 8 от 29 июня 2017 г.) http://docspace.kubsu.ru/docspace/handle/1/1119 Методические указания по выполнению самостоятельной работы обучающихся (Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 8 от 29 июня 2017 г.) http://docspace.kubsu.ru/docspace/handle/1/1126

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
– в печатной форме увеличенным шрифтом,
– в форме электронного документа,
Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии

В процессе изучения дисциплины лекции, практические занятия, консультации являются ведущими формами обучения в рамках лекционно-семинарской образовательной технологии.

Лекции излагаются в виде презентации с использованием мультимедийной аппаратуры. Данные материалы в электронной форме передаются студентам.

Основной целью практических занятий является разбор практических ситуаций. Дополнительной целью практических занятий является контроль усвоения пройденного материала. На практических занятиях также осуществляется проверка выполнения заданий.

При проведении практических занятий участники готовят и представляют (с использованием программы Power Point) небольшие сообщения по наиболее важным теоретическим аспектам текущей темы, отвечают на вопросы преподавателя и других слушателей. В число видов работы, выполняемой слушателями самостоятельно, входят: 1) поиск и изучение литературы по рассматриваемой теме; 2) поиск и анализ научных статей, монографий по рассматриваемой теме; 3) подготовка реферативных обзоров; 4) подготовка презентации.

Интерактивные образовательные технологии, используемые в аудиторных занятиях: при реализации различных видов учебной работы (лекций и практических занятий) используются следующие образовательные технологии: дискуссии, презентации, конференции. В сочетании с внеаудиторной работой они создают дополнительные условия формирования и развития требуемых компетенций обучающихся, поскольку позволяют обеспечить активное взаимодействие всех участников. Эти методы способствуют личностно-ориентированному подходу.

Для инвалидов и лиц с ограниченными возможностями здоровья устанавливается особый порядок освоения указанной дисциплины. В образовательном процессе используются социально-активные и рефлексивные методы обучения (ролевая игра), технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Вышеозначенные образовательные технологии дают наиболее эффективные результаты освоения дисциплины с позиций актуализации содержания темы занятия, выработки продуктивного мышления, терминологической грамотности и компетентности обучаемого в аспекте социально-направленной позиции будущего специалиста, и мотивации к инициативному и творческому освоению учебного материала.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

4.1 Фонд оценочных средств для проведения текущей аттестации

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Примерные темы рефератов (презентаций) (ПК-9; ПК-11)

1. Безопасность информационных технологий
2. Безопасность информационных технологий и расследование компьютерных инцидентов
3. Безопасность информационных технологий и сетей
4. Безопасность информационных технологий на основе операционных систем Windows
5. Безопасность компьютерных сетей
6. Безопасность сетей на базе Linux (Unix)
7. Защита информации
8. Топ 10 угроз информационной безопасности на предприятии
9. Необходимость защиты информации
10. Основные законодательные и нормативные акты регулирующие вопросы безопасности в сфере профессиональной деятельности
11. Информационная безопасность и медиа-культура
12. Технологии и средства обеспечения компьютерной безопасности
13. Система национальной безопасности Российской Федерации
14. Угроза постиндустриального мира
15. Составляющие информационной безопасности
16. Индикативная система экономической безопасности
17. Основы информационной безопасности
18. Современные методологии оценки рисков информационной безопасности
19. Защита интеллектуальной собственности
20. Способы кодирования и декодирования информации
21. Основы защиты информации в телекоммуникационных системах
22. Информационная безопасность предприятия
23. Экологическая безопасность и особенность её обеспечения
24. История возникновения систем компьютерной математики и её возможности в наше время и в 1960 гг.

25. Ценности, нормы и правила в научной среде. Нравственная ответственность учёного.
26. Источники научной информации, поиск её по теме исследования, обработка найденных результатов
27. Виды и формы представления информации
28. Информационная безопасность
29. Создание комплексной системы защиты информации на предприятии
30. Типовая структура технического канала утечки информации
31. Технические аспекты защиты информации
32. Симметричные криптосистемы шифрования
33. Необходимость защиты информации
34. Объект, предмет, методология, теория и практика безопасности
35. Интеллектуальная и кадровая безопасность предприятия
36. Технико-технологическая безопасность предприятия
37. Система защиты информации администрации округа N г. Краснодара
38. Информационная безопасность в ОВД
39. Информационная безопасность и ее составляющие
40. Информационная безопасность личности, общества, государства
41. Информационная безопасность предприятия
42. Использование SEO-оптимизации для оценки уязвимости портальных решений
43. Информационная безопасность предприятия
44. Обучение пользователей на этапе внедрения ИС
45. Защита информации в локальных компьютерных сетях от несанкционированного доступа
46. Правовое регулирование в области информационных ресурсов
47. Методы машинного обучения в информационной безопасности информационных систем
48. Современное состояние развития теории информационной безопасности
49. Требования, предъявляемые к конфиденциальности информации
50. Оптимизация web-сервера
51. Юридические особенности и свойства информации
52. Создание доверенных информационных систем: способы построения
53. Проблемы информационной безопасности в вычислительных сетях
54. Требования к концепции защиты информации
55. Законодательные и нормативные документы по защите авторских прав.(методология)
56. Программные средства защиты информации
57. Анализ нормативной базы в области информационной безопасности в РФ
58. Внешние факторы, влияющие на состояние национальной безопасности Российской Федерации
59. Классификация и характеристика объектов защиты информации
60. Рынок информационных технологий
61. Содержание и организация процесса аудита информационной безопасности организации
62. Вирусы и антивирусные программы
63. Защита информации в системах реального времени
64. История развития защиты информации

65. Установка ПО ИБ на предприятии
66. Субъекты управления информационной безопасности организаций, их функции, права и обязанности
67. Электронная цифровая подпись
68. Информационная безопасность коммерческого предприятия
69. Основы безопасной работы в интернете
70. Что такое вирусная атака ? Физический механизм реализации
71. Асимметричные криптосистемы
72. Целостность информации
73. Информационная безопасность в сфере государственного управления
74. Криптография электронного голосования
75. Требования к информационно-аналитической системе службы безопасности
76. Стандарты информационной безопасности
77. Основы защиты информации в телекоммуникационных системах
78. Вирусные атаки и методы защиты от них
79. Сравнительный анализ Dr.WEB enterprise security suite 10 и Kaspersky Endpoint Security 10
80. Авторское право в Internet
81. Механизмы защиты информации в вычислительных сетях
82. Нормативно-правовые аспекты защиты информации
83. Назначение и особенности применения технических средств обнаружения проникновения посторонних лиц на объект
84. Защита информации
85. Вирусные атаки и методы защиты от них
86. Информационные системы органов исполнительной власти
87. Уголовная и административная ответственность за разглашение сведений ограниченного доступа и проблемы информационной безопасности

Примерный перечень контрольных вопросов по отдельным темам дисциплины «Информационная безопасность» для направления 38.03.05 «Бизнес-информатика» профиль «Электронный бизнес» (ПК-9; ПК-11)

1.Понятие "информационная безопасность"
2. Составляющие информационной безопасности
3. Система формирования режима информационной безопасности
4.Нормативно-правовые основы информационной безопасности в РФ
5.Стандарты информационной безопасности: "Общие критерии"
6.Стандарты и спецификации в области информационной безопасности
7.Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт
8.Информационная безопасность распределённых систем. Рекомендации X.800
9.Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
10.Гармонизированные критерии Европейских стран
11.Интерпретация «Оранжевой книги» для сетевых конфигураций. Руководящие документы Гостехкомиссии России
12.Государственная политика информационной безопасности
13.Органы обеспечения информационной безопасности
14.Причины возникновения проблем с ИТ-безопасностью

15. Значимость различных проблем ИТ-безопасности
16.Программные средства контроля доступа
17. Средства контроля доступа к документам в MS Office
18. Контроль доступа к Web-ресурсу
19. Аппаратные средства контроля доступа
20.Биометрические средства контроля доступа
21.Криптография
22.Шифрование с помощью ключа
23.Шифрование с симметричным ключом;
24.Асимметричное шифрование;
25.Шифрование с симметричным и асимметричным ключом.
26.Цифровые сертификаты. Классы сертификатов.
27.Система подписанных приложений.
28.Безопасность при переписке
29.Лицензирование деятельности в области информационной безопасности
30.Общая характеристика технического канала утечки информации
31.Классификация технических каналов утечки информации, обрабатываемой техническими средствами передачи информации
32.Классификация технических каналов утечки речевой информации
33.Классификация технических каналов перехвата информации при её передаче по каналам связи
34.Общие принципы и методы выявления технических каналов утечки информации
35.Индикаторы поля, интерсепторы и измерители частоты
36.Специальные сканирующие радиоприёмники
37.Обнаружители диктофонов
38.Универсальные поисковые приборы
39.Программно-аппаратные поисковые комплексы
40.Технические средства контроля двухпроводных линий
41.ФЗ «Об информации, информационных технологиях и о защите информации».
42.Информация, запрещённая к распространению в СМИ, а также в компьютерных сетях.
43.Государственная тайна.
44.Правовой базис института государственной тайны.
45.Режим государственной тайны.
46.Перечень сведений, составляющих государственную тайну.
47.Сведения, не подлежащие отнесению к государственной тайне и засекречиванию.
48.Органы государственно-правового регулирования информационных отношений в области государственной тайны.
49.Допуск граждан к государственной тайне.
50.Классификация технических средств выявления каналов утечки информации
51.Степени секретности сведений.
52.Объективная сторона состава государственной измены.
53.Огласка сведений, составляющих государственную тайну.
54.Понятие Защиты информации.
55.Государственное регулирование защиты информации.
56.Субъекты защиты информации.
57.Обладатель информации.
58.Оператор информационной системы.
59.Требования о защите информации, содержащейся в ГИС.
60.Ответственность за правонарушения.

61.Документирование информации.
62.Сетевые модели передачи данных
63.Модель взаимодействия открытых систем OSI/ISO
64.Адресация в глобальных сетях
65.Классификация удаленных угроз в вычислительных сетях
66.Типовые удаленные атаки и их характеристика

Примеры тестовых заданий (ПК-9; ПК-11)

1.Установите соответствие дефиниций с их содержанием

№№ п/п	Наименование дефиниции	№№ п/п	Содержание дефиниции
1.	В Доктрине информационной безопасности Российской Федерации термин "информационная безопасность" - это	А.	защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.
2.	В Законе РФ "Об информации, информационных технологиях и о защите информации" информационная безопасность определяется как	Б.	актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.
3.	Информационная безопасность в учебнике Галатенко В.А.	В.	это комплекс мероприятий, направленных на обеспечение информационной безопасности.
4.	Защита информации - это	Г.	состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.
5.	Доступность - это	Д.	основа современной технологии программирования, испытанный метод борьбы со сложностью систем.
6.	Целостность - это	Е.	состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.
7.	Конфиденциальность - это	Ж.	элемент класса, то есть абстракция определенной сущности.
8.	Объектно-ориентированный подход к информационной безопасности - это	З.	возможность за приемлемое время получить требуемую информационную услугу.
9.	Класс - это	И.	абстракция множества сущностей реального мира, объединенных общностью структуры и поведения.
10.	Объект - это	К.	защита от несанкционированного доступа к инфор-

			мации.

2 Тестовые задания открытой формы

2.1. Закончите предложение.

2.1.1. Чтобы рассматривать ИС предметно, с использованием актуальных данных, следует составить …… …… ……

2.1.2. Результаты оценки критичности являются отправной точкой в составлении ……

2.1.3. Первый шаг в анализе угроз - их……

2.1.4. Управление рисками, как и любую другую деятельность в области информационной безопасности, необходимо интегрировать в жизненный цикл…… ……

2.1.5. Если какие-либо риски оказались недопустимо высокими, необходимо их нейтрализовать, реализовав дополнительные …… ……

2.1.6. Меры физического управления доступом позволяют контролировать и при необходимости ограничивать …… и …… сотрудников и посетителей

2.1.7. Оценивая стоимость мер защиты, приходится учитывать не только прямые расходы на закупку оборудования и/или программ, но и расходы на ее ……

2.1.8. Программа безопасности, принятая организацией, должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима …… ……

2.1.9. Меры информационной безопасности можно разделить на три группы, в зависимости от того, направлены ли они на предупреждение, обнаружение или ликвидацию последствий ……

2.1.10. Стратегия восстановительных работ должна предусматривать не только работу по временной схеме, но и возвращение к …… ……

2.2. Впишите пропущенное слово.

2.2.1. С практической точки зрения политику безопасности целесообразно рассматривать на ……уровнях детализации.

2.1.2. Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и ……

2.1.3. В жизненном цикле информационного сервиса можно выделить следующие этапы: инициация, закупка, установка, …… и выведение из эксплуатации.

2.1.4. Результаты оценки …… являются отправной точкой в составлении спецификаций.

2.1.5. Если данные архивируются в зашифрованном виде, необходимо сохранить…… и средства расшифровки.

2.1.6. По отношению к выявленным рискам возможны следующие действия: …… риска, уменьшение риска, принятие риска, переадресация риска.

2.1.7. При идентификации активов, то есть тех ресурсов и ценностей, которые организация пытается защитить, следует учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, такие как…… организации.

2.1.8. Предварительное составление описания должности позволяет оценить ее …… и спланировать процедуру проверки и отбора кандидатов.
2.1.9. Поддержка пользователей подразумевает прежде всего …… и оказание помощи при решении разного рода проблем.
2.2.10. Программа…… , принятая организацией, должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима информационной безопасности.

3.Определение объекта по краткой характеристике, ответ необходимо вписать самостоятельно

3.1. Строится на основе анализа рисков, которые признаются реальными для информационной системы организации - …….. …….
3.2. Должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь - …….. ……. ……..
3.3. Она включает в себя два аспекта - цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации - …….. ……. ……..
3.4. На данном этапе нужно окончательно сформулировать требования к защитным средствам нового сервиса, к компании, которая может претендовать на роль поставщика, и к квалификации, которой должен обладать персонал, использующий или обслуживающий закупаемый продукт - …….. ……. .
3.5. Необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки - …….. ……. ……..
3.6. Практически все этапы этого процесса связаны между собой, и по завершении почти любого из них может возникнуть необходимость возврата к предыдущему -…….. …….
3.7. Принцип, который предписывает так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс - принцип …….. ……. .
3.8. Системы электро-, водо- и теплоснабжения, кондиционеры и средства коммуникаций можно отнести к …….. …….
3.9. Компьютеры, программы и данные, информационные сервисы внешних организаций, документация являются элементами …….. ……. .
3.10. Здания, инженерные коммуникации, средства связи, оргтехника относятся к …….. ……. .

4.Найдите правильный(е) вариант(ы) ответа(ов)

4.1. К граням вредоносного ПО относится(ятся):

А. вредоносная функция;

Б. способ распространения;

В. внутреннее представление;

Г. внешнее представление.

1.Верно только А и Б. 2.Верно А и Б, Г. 3.Верно только Б. 4.Все суждения неверны. 5. Все суждения верны.

4.2. По механизму распространения различают:

А. вирусы ;

Б."черви" ;

В. Трояны.

1.Верно только А. 2.Верно А и Б. 3.Верно только Б. 4.Все суждения неверны.

4.3. Вирусы – это:
А. код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы
Б. код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;
В. Код, способный с помощью других вспомогательных устройств вызывать распространение своих копий по ИС и их выполнение.
1.Верно только А и Б. 2.Верно Б и В.. 3.Верно только Б. 4.Все суждения неверны.
4.4. Вирусы обычно распространяются:
А. локально
Б. в пределах узла сети
В. В пределах одного компьютера
1.Верно только А и Б. 2.Верно Б и В.. 3.Верно только Б. 4.Все суждения неверны.
4.5. Вредоносный код, который выглядит как функционально полезная программа, называется:
А. троянским
Б. вредоносный кодом прямого действия
В. Вирусом
1.Верно только А и Б. 2.Верно Б и В.. 3.Верно только А. 4.Все суждения неверны
4.6. С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:
А. ввести неверные данные;
Б. изменить данные;
В. Украсть информацию;
Г. открыть доступ 3-им лицам к информации.
1.Верно только А и Б. 2.Верно Б и В.. 3.Верно только А и Г. 4.Все суждения неверны
4.7. Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и:
А. программы
Б. программные данные
В. Данные о программах
1.Верно только А и Б. 2.Верно А.. 3.Верно только А и В. 4.Все суждения неверны
4.8. маскарад –это :
А. выполнение действий под видом лица, обладающего полномочиями для доступа к данным;
Б. выполнение программ под видом лица, обладающего полномочиями для доступа к данным;
В. Невыполнение действий под видом лица, обладающего полномочиями для доступа к данным.
1.Верно только А и Б. 2.Верно А и В. 3.Верно только А. 4.Все суждения неверны
4.9. Угрозы можно классифицировать по нескольким критериям:
А. по аспекту информационной безопасности, против которого угрозы направлены в первую очередь;
Б. по компонентам информационных систем, на которые угрозы нацелены
В. по способу осуществления ;
Г. по расположению источника угроз;
1.Верно только А и Б. 2.Верно А и В. 3.Верно только А. 4.Все суждения неверны. 5. Все суждения верны

4.10. Объект – это:

А. абстракция множества сущностей реального мира, объединенных общностью структуры и поведения.

Б. это элемент класса, то есть абстракция определенной сущности;

В. сокрытие реализации объектов (их внутренней структуры и деталей реализации методов) с предоставлением вовне только строго определенных интерфейсов;

Г. это элемент семейства, т.е. определенный класс в развитии.

1.Верно только А и Б. 2.Верно А и В. 3.Верно только Б и В. 4.верно только Б. 5. Все суждения верны

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Вопросы для экзамена по дисциплине (ПК-9; ПК-11).

1.Понятие "информационная безопасность"
2. Составляющие информационной безопасности
3. Система формирования режима информационной безопасности
4.Нормативно-правовые основы информационной безопасности в РФ
5.Стандарты информационной безопасности: "Общие критерии"
6.Стандарты и спецификации в области информационной безопасности
7.Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт
8.Информационная безопасность распределённых систем. Рекомендации X.800
9.Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
10.Гармонизированные критерии Европейских стран
11.Интерпретация «Оранжевой книги» для сетевых конфигураций. Руководящие документы Гостехкомиссии России
12.Государственная политика информационной безопасности
13.Органы обеспечения информационной безопасности
14.Причины возникновения проблем с ИТ-безопасностью
15. Значимость различных проблем ИТ-безопасности
16.Программные средства контроля доступа
17. Средства контроля доступа к документам в MS Office
18. Контроль доступа к Web-ресурсу
19. Аппаратные средства контроля доступа
20.Биометрические средства контроля доступа
21.Криптография
22.Шифрование с помощью ключа
23.Шифрование с симметричным ключом;
24.Асимметричное шифрование;
25.Шифрование с симметричным и асимметричным ключом.
26.Цифровые сертификаты. Классы сертификатов.
27.Система подписанных приложений.
28.Безопасность при переписке
29.Лицензирование деятельности в области информационной безопасности
30.Общая характеристика технического канала утечки информации
31.Классификация технических каналов утечки информации, обрабатываемой техническими средствами передачи информации
32.Классификация технических каналов утечки речевой информации
33.Классификация технических каналов перехвата информации при её передаче по каналам связи

34.Общие принципы и методы выявления технических каналов утечки информации
35.Индикаторы поля, интерсепторы и измерители частоты
36.Специальные сканирующие радиоприёмники
37.Обнаружители диктофонов
38.Универсальные поисковые приборы
39.Программно-аппаратные поисковые комплексы
40.Технические средства контроля двухпроводных линий
41.ФЗ «Об информации, информационных технологиях и о защите информации».
42.Информация, запрещённая к распространению в СМИ, а также в компьютерных сетях.
43.Государственная тайна.
44.Правовой базис института государственной тайны.
45.Режим государственной тайны.
46.Перечень сведений, составляющих государственную тайну.
47.Сведения, не подлежащие отнесению к государственной тайне и засекречиванию.
48.Органы государственно-правового регулирования информационных отношений в области государственной тайны.
49.Допуск граждан к государственной тайне.
50.Классификация технических средств выявления каналов утечки информации
51.Степени секретности сведений.
52.Объективная сторона состава государственной измены.
53.Огласка сведений, составляющих государственную тайну.
54.Понятие Защиты информации.
55.Государственное регулирование защиты информации.
56.Субъекты защиты информации.
57.Обладатель информации.
58.Оператор информационной системы.
59.Требования о защите информации, содержащейся в ГИС.
60.Ответственность за правонарушения.
61.Документирование информации.
62.Сетевые модели передачи данных
63.Модель взаимодействия открытых систем OSI/ISO
64.Адресация в глобальных сетях
65.Классификация удаленных угроз в вычислительных сетях
66.Типовые удаленные атаки и их характеристика

5.Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

5.1 Основная литература:*

1. Партыка, Т. Л. Информационная безопасность [Электронный ресурс] : учебное пособие / Т. Л. Партыка, И. И. Попов. - 5-е изд,. перераб. и доп. - Москва: ФОРУМ : ИНФРА-М, 2016. - 432 с. - http://znanium.com/bookread2.php?book=516806.

2. Нестеров, С. А. Информационная безопасность [Электронный ресурс] : учебник и практикум для академического бакалавриата / С. А. Нестеров. - М. : Юрайт, 2017. - 321 с. - https://www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7.

3.Внуков, А.А. Защита информации: учебное пособие для бакалавриата и магистратуры/А.А.Внуков. — 2-е изд., испр. и доп. — М.: Издательство Юрайт, 2017. — 261 с. — (Серия: Бакалавр и магистр. Академический курс).— ISBN 978-5-534-01678-9.

4.Внуков, А.А. Защита информации в банковских системах: учебное пособие для бакалавриата и магистратуры / А.А.Внуков. — 2-е изд., испр. и доп. — М.: Издательство

Юрайт, 2017. —246 с. — (Серия: Бакалавр и магистр. Академический курс). – ISBN 978-5-534-01679-6.

5.2 Дополнительная литература:

5.Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л.К.Бабенко, Е.А.Ищукова. — М.: Издательство Юрайт, 2017. — 220 с. — (Серия: Университеты России). — ISBN 978-5-9916-9244-1.

6.Галатенко, В. А. Основы информационной безопасности: учеб. пособие для вузов / В. А. Галатенко. – 4-е изд. – М.: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2012. – 205 с. – (Сер. "Основы информационных технологий") . - ISBN 978-5-947748-21-5.

7.Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации. СПб.: СПбГУ ИТМО, 2010. - 98 с

*Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

5.3. Периодические издания:

1. Вопросы экономики
2. Деньги и кредит
3. Computerra.
4. Российский экономический журнал
5. Финансовые известия
6. Экономика и жизнь
7. Экономист
8. Эксперт

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Для самостоятельной работы студентам рекомендуется обращаться к текущим публикациям и информации, помещаемой на следующих сайтах Интернет:

1. http://www.akdi.ru – Агентство консультаций и деловой информации «Экономика».
2. http://www.eeg.ru – макроэкономическая статистика России на сайте экспертной группы Министерства финансов РФ.
3. http://www.nns.rn/analytdoc/ana12.html − аналитические доклады по экономическим проблемам России на сайте «Национальной электронной библиотеки».
4. http://www/libertarium.ru/libertarium/library − библиотека Либертариума, где представлены книги и статьи по экономическим наукам, а также труды выдающихся экономистов прошлого и современности;
5. http://www.econline.hl.ru – коллекция ссылок на лучшие экономические ресурсы Сети, как англо-, так и русскоязычные. Сайт охватывает широкий круг экономических дисциплин: экономические новости, микроэкономика, макроэкономика, математические методы в экономике, методология и история экономической мысли, институциональная экономика, Интернет-экономика, международная экономика, экономическая статистика и др.
6. http:// www.beafnd.org – Фонд «Бюро экономического анализа» (г. Москва).
7. http://www.cbr.ru – Центральный банк Российской Федерации.
8. http://www.imf.org – Международный валютный фонд.
9. http://www.economy.gov.ru – Министерство экономического развития и торговли РФ.
10. http://www.csr.ru – Центр стратегических разработок.

11. http://www.ecsocman.edu.ru – Федеральный образовательный портал – ЭКОНОМИКА, СОЦИОЛОГИЯ, МЕНЕДЖМЕНТ – учебные материалы.

Кроме того, рекомендуется пользоваться электронными ресурсами библиотеки Кубанского государственного университета.

7. Методические указания для обучающихся по освоению дисциплины (модуля).

Самостоятельная работа слушателей по дисциплине «Информационная безопасность» проводится с целью закрепления и систематизации теоретических знаний, формирования практических навыков по их применению при решении экономических задач в выбранной предметной области. Самостоятельная работа включает: изучение основной и дополнительной литературы, проработка и повторение лекционного материала, материала учебной и научной литературы, подготовку к практическим занятиям, подготовка рефератов (презентаций), подготовка к тестированию и исследовательской работе (ИР).

Для подготовки к лекциям необходимо изучить основную и дополнительную литературу по заявленной теме и обратить внимание на те вопросы, которые предлагаются к рассмотрению в конце каждой темы.

При изучении основной и дополнительной литературы, студент может в достаточном объеме усвоить и успешно реализовать конкретные знания, умения, навыки и компетенции при выполнении следующих условий:

1) систематическая работа на учебных занятиях под руководством преподавателя и самостоятельная работа по закреплению полученных знаний и навыков;

2) добросовестное выполнение заданий преподавателя на практических занятиях;

3) выяснение и уточнение отдельных предпосылок, умозаключений и выводов, содержащихся в учебном курсе; взаимосвязей отдельных его разделов, используемых методов, характера их использования в практической деятельности менеджера;

4) сопоставление точек зрения различных авторов по затрагиваемым в учебном курсе проблемам; выявление неточностей и некорректного изложения материала в периодической и специальной литературе;

5) разработка предложений преподавателю в части доработки и совершенствования учебного курса;

6) подготовка научных статей для опубликования в периодической печати, выступление на научно-практических конференциях, участие в работе студенческих научных обществ, круглых столах и диспутах по антикоррупционным проблемам.

В ходе самоподготовки к практическим занятиям студент осуществляет сбор и обработку материалов по тематике его исследования, используя при этом открытые источники информации (публикации в научных изданиях, аналитические материалы, ресурсы сети Интернет и т.п.), а также практический опыт и доступные материалы объекта исследования. Контроль за выполнением самостоятельной работы проводится при изучении каждой темы дисциплины на практических (семинарских) занятиях.

Важнейшим элементом самостоятельной работы является подготовка к написанию исследовательской работы. Этот вид самостоятельной работы позволяет углубить теоретические знания и расширить практический опыт студента, его способность генерировать собственные идеи, умение выслушать альтернативную точку зрения, аргументированно отстаивать свою позицию, сформировать командные навыки принятия решений.

На сегодняшний день тестирование – один из самых действенных и популярных способов проверить знания в изучаемой области. Тесты позволяют очень быстро проверить наличие знаний у студентов по выбранной теме. Кроме того, тесты не только проверяют знания, но и тренируют внимательность, усидчивость и умение быстро ориентиро-

ваться и соображать. При подготовке к решению тестов необходимо проработать основные категория и понятия дисциплины, обратить внимание на ключевые вопросы темы.

Подготовка реферата (презентации) – закрепление теоретических основ и проверка знаний студентов по вопросам основ и практической организации научных исследований, умение подбирать, анализировать и обобщать материалы, раскрывающие связи между теорией и практикой. Подготовка презентации предполагает творческую активность слушателя, умение работать с литературой, владение методами анализа данных и компьютерными технологиями их реализации.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю).

8.1 Перечень необходимого программного обеспечения.

При освоении всех тем дисциплины необходимо следующее ПО: Microsoft Windows 8, 10; Microsoft Office Professional Plus.

8.2 Перечень необходимых информационных справочных систем

1. http://www.elibrary.ru)/ - Электронная библиотечная система eLIBRARY.RU
2. www.biblioclub.ru Электронная библиотечная система «Университетская библиотека ONLINE».
3. www.e.lanbook.com Электронная библиотечная система издательства «Лань».
4. http://www.biblio-online.ru/ Электронная библиотечная система "Юрайт".
5. **www.znanium.com** Электронная библиотечная система "ZNANIUM.COM".
6. https://www.book.ru Электронная библиотечная система "BOOK.ru"

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

№	Наименование специальных помещений и помещений для самостоятельной работы	Номера аудиторий / кабинетов
1.	Учебные аудитории для занятий лекционного типа	Ауд. 201А, 202А, 205А, 520А, 207Н, 208Н, 209Н, 212Н, 214Н, 2026Л, 2027Л, 4033Л, 4034Л, 4035Л, 4036Л, 4038Л, 4039Л, 5040Л, 5041Л, 5042Л, 5045Л, 5046Л
2.	Учебные аудитории для проведения занятий семинарского типа	А208Н, 210Н, 216Н, 513А, 514А, 515А, 516А, 5043Л 201А, 202А, 205А, 520А, 2026Л, 2027Л, 4033Л, 4034Л, 4035Л, 4036Л, 4038Л, 4039Л, 5040Л, 5041Л, 5042Л, 5045Л,

		5046Л, 207Н, 208Н, 209Н, 212Н, 214Н,
3.	Аудитории для групповых и индивидуальных консультаций	Кафедра Теоретической экономики ауд. 230
4.	Аудитории для проведения текущего контроля и промежуточной аттестации	А208Н, 210Н, 216Н, 513А, 514А, 515А, 516А, 5043Л 201А, 202А, 205А, 520А, 201Н, 202Н, 203Н, А203Н, 207Н, 208Н, 209Н, 212Н, 214Н, 2026Л, 2027Л, 4033Л, 4034Л, 4035Л, 4036Л, 4038Л, 4039Л, 5040Л, 5041Л, 5042Л, 5045Л, 5046Л
5.	Помещения для самостоятельной работы, с рабочими местами, оснащенными компьютерной техникой с подключением к сети «Интернет» и обеспечением неограниченного доступа в электронную информационно-образовательную среду организации для каждого обучающегося, в соответствии с объемом изучаемых дисциплин	Ауд. 201Н, 202Н, 213А, 218А

Перечень необходимых информационных справочных систем и профессиональных баз данных

Обучающимся обеспечен доступ к современным профессиональным базам данных, профессиональным справочным и поисковым системам:

1. Консультант Плюс - справочная правовая система http://www.consultant.ru;
2. База данных международных индексов научного цитирования Web of Science (WoS) http://webofscience.com/;
3. База данных рефератов и цитирования Scopus http://www.scopus.com/;
4. Базы данных компании «Ист Вью» http://dlib.eastview.com;
5. База открытых данных Росфинмониторинга http://fedsfm.ru/opendata;
6. База открытых данных Росстата http://www.gks.ru/opendata/dataset;
7. База открытых данных Управления Федеральной службы государственной статистики по Краснодарскому краю и Республике Адыгея http://krsdstat.gks.ru/wps/wcm/connect/rosstat_ts/krsdstat/ru/statistics/krsndStat/db/;
8. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/;
9. Электронная Библиотека Диссертаций https://dvs.rsl.ru;
10. Научная электронная библиотека КиберЛенинка http://cyberleninka.ru/