1920

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
филиал Федерального государственного бюджетного образовательного
учреждения высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
в г. Новороссийске
Кафедра информатики и математики

УТВЕРЖДАЮ
Проректор по работе с филиалами
ФГБОУ ВО «Кубанский
государственный университет»
_____ А.А.Евдокимов
«31» 08 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.09 Обеспечение безопасности электронного бизнеса

Направление подготовки: 38.03.05 Бизнес-информатика

Направленность (профиль): Электронный бизнес

Программа подготовки академическая

Форма обучения очная

Квалификация (степень) выпускника бакалавр

Год начала подготовки 2015
Краснодар 2016

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 38.03.05 Бизнес-информатика, утвержденного приказом Министерства образования и науки Российской Федерации № 1002 от 11 августа 2016 года.

Программу составил(и):

И.Г.Рзун, доцент канд.физ.-мат.наук

С.В. Дьяченко доцент канд.физ.-мат.наук

Рабочая программа дисциплины утверждена на заседании кафедры информатики и математики
протокол № 1 от 29.08.2016 г.

Заведующий кафедрой (разработчика) Рзун И.Г

Рабочая программа обсуждена на заседании кафедры информатики и математики
протокол № 1 от 29.08.2016 г.

Заведующий кафедрой (выпускающей) Рзун И.Г.

Рабочая программа одобрена на заседании учебно-методической комиссии филиала по УГСН 01.00.00 Математика и механика
протокол № 1 29.08.2016 г.

Председатель УМК С.В. Дьяченко

Рецензенты:

Адамович А.Е., Директор ООО «Финам - Новороссийск»

Кунина М.К., Директор по развитию ООО «АЙТИ БИЗНЕС ЮГ»

Содержание рабочей программы дисциплины

1 Цели и задачи изучения дисциплины.

1.1 Цель освоения дисциплины.

Цель изучения курса Б1.В.09 «Обеспечение безопасности электронного бизнеса» - добиться всестороннего и глубокого понимания студентами природы сущности спектра отношений, возникающих в процессе функционирования реального хозяйствующего субъекта(отношения управления, координации, кооперации, конкуренции, агрессивного соперничества, торгово- экономической войны) как определяющего фактора обеспечения эффективности работы организации на всех уровнях и во всех реальных ракурсах.

1.2 Задачи дисциплины.

Обеспечение безопасности электронного бизнеса (ОБЭБ) (информационная безопасность (ИБ) органично включается в этот комплекс своим технико-технологическим содержанием) - сравнительно молодая, быстро развивающаяся область информационных технологий (ИТ), для успешного освоения которой важно с самого начала усвоить современный, согласованный с другими ветвями ИТ базис. Это - первая задача курса, для решения которой привлекается объектно- ориентированный подход. Успех в области ОБЭБ может принести только комплексный подход. Описание общей структуры и отдельных уровней такого подхода - вторая задача курса. Для её решения рассматриваются меры законодательного, административного, процедурного и программно-технического уровней. Приводятся сведения о российском и зарубежном законодательстве в области ОБЭБ, о проблемах, существующих в настоящее время в российском законодательстве. На административном уровне рассматриваются политика и программа безопасности, их типовая структура, меры по выработке и сопровождению. На процедурном уровне описываются меры безопасности, имеющие дело с людьми. Формулируются основные принципы, помогающие успеху таких мер. Программно-технический уровень, в соответствии с объектным подходом, трактуется как совокупность сервисов. Даётся описание каждого сервиса.

В ходе изучения дисциплины ставятся задачи:

– выработка умения моделировать реальные экономические процессы;

– развитие логического и алгоритмического мышления обучающихся;

– повышение уровня математической культуры обучающихся;

–подготовка отчетов, обзоров;

– поиск, сбор, обработка и систематизация информации об экономике и ИКТ.

1.3 Место дисциплины в структуре образовательной программы.

Дисциплина «Обеспечение безопасности электронного бизнеса» (далее – дисциплина) находится в вариативной части дисциплин по выбору учебного плана. Приступая к изучению данной дисциплины, студент должен иметь базовые знания по курсам : «Развитие информационного общества», «Теоретические основы информатики», «Моделирование бизнес-процессов», «Вычислительные системы, сети, телекоммуникации».

Знания и умения, полученные в результате освоения дисциплины «Обеспечение безопасности электронного бизнеса», являются необходимыми для прохождения производственной практики и подготовки выпускной квалификационной работы.

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

Процесс изучения дисциплины направлен на формирование следующих общекультурных и профессиональных компетенций: ОПК-1, ПК-7, ПК -9, ПК-21

№ п.п.	Индекс компет	Содержание компетенции (или её	В результате изучения учебной дисциплины обучающиеся должны

	енции	части)	**знать**	**уметь**	**владеть**
1.	ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	- о требованиях ИБ в области профессиональной деятельности. - современные тенденции развития в области техники и технологий.	**Уметь:** -определять набор требований по защите информации в текущих условиях. - учитывать тенденции развития техники связи в своей деятельности.	-навыком поиска необходимых РД. - навыками работы с Российской и зарубежной научно-исследовательской литературой по тематике.
2	ПК-7	использование современных стандартов и методик, разработка регламентов для организации управления процессами жизненного цикла ИТ-инфраструктуры предприятий	-современные стандарты деятельности предприятия -современные стандарты и методики, регламенты деятельности предприятия -современные методы, средства, стандарты информатики для решения прикладных задач различных классов; современные методологии и технологии проектирования ИС; стандарты и	разрабатывать регламенты деятельности предприятия -использовать современные стандарты и методики, разрабатывать регламенты деятельности предприятия -выбирать методологию и технологию проектирования ИС; применять современные методы управления проектами и сервисами ИС; разрабатывать регламенты деятельности	-методами применения стандартов для разработки регламентов. -инструментарием управления проектами создания, внедрения и развития ИС -навыками формулирования требований к ИС; навыками проектирования информационных систем с использованием современных

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
			методы планирования проектов -основные стадии и этапы жизненного цикла информационной системы; структуру информационной системы; методы разработки структуры информационной системы	предприятия -определять стадии и этапы жизненного цикла информационной системы; разрабатывать структуру информационной системы	инструментальных средств; навыками организации экспертиз и выбора решений. -опытом проектирования информационной системы, использования структурного программирования и модульного программирования
3	ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	-о принципах управления ИБ	-определять способы взаимодействия с клиентами и партнерами с учетом требований ИБ	-навыком минимизации рисков ИБ при взаимодействии с клиентами и партнерами
4	ПК-21	умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия	-о принципах управления ИБ ИТ-инфраструктуры предприятия.	консультировать заказчиков по вопросам совершенствования управления ИБ ИТ-инфраструктуры предприятия.	-навыками определения приоритетных вопросов в области управления ИБ ИТ-инфраструктуры предприятия.

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет _4__ зач.ед. (__144__ часов), их распределение по видам работ представлено в таблице

Вид учебной работы		Всего часов	Семестры (часы)			
			7			
Контактная работа, в том числе:		**56,2**	**56,2**			
Аудиторные занятия (всего):		**50**	**50**			
Занятия лекционного типа		18	18		-	-
Лабораторные занятия					-	-
Занятия семинарского типа (семинары, практические занятия)		32	32		-	-
		-	-		-	-
Иная контактная работа:		**6,2**	**6,2**			
Контроль самостоятельной работы (КСР)		6	6			
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:		**87,8**	**87,8**			
Курсовая работа		-	-		-	-
Проработка учебного (теоретического) материала		53,8	53,8		-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		30	30		-	-
Реферат		4	4		-	-
Подготовка к текущему контролю					-	-
Контроль:						
Подготовка к экзамену		27	27			
Общая трудоемкость	**час.**	**144**	**144**		-	-
	в том числе контактная работа	**56,2**	**56,2**			
	зач. ед	**4**	**4**			

Курсовые не предусмотрены.

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 7 семестре

№	Наименование разделов	Количество часов					
		Всего	Контактная работа				Самостоятельная работа
			Л	ПЗ	ИКР	КСР	СР
1.	Основные модели электронной коммерции. Угрозы безопасности электронной коммерции и электронных платежей.	29	3	7		2	17
2.	Политика информационной безопасности. Построение систем безопасности электронного бизнеса.	28	4	6			18
3.	Методы и средства обеспечения информационной безопасности электронного бизнеса	29	3	7		2	17
4	Корпорат ивные стандарты обеспечения информационной безопасности систем.	**28**	**4**	**6**			**18**
5	Развитие информационно-коммуникационных технологий	**29,8**	**4**	**6**		**2**	**17,8**
	Итого по дисциплине	**143,8**	**18**	**32**		**6**	**87,8**
	Промежуточная аттестация (ИКР)	0,2			0,2		
	Всего:	144	18	32	0,2	6	87,8

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, КСР – контролируемая самостоятельная работа, СР – самостоятельная работа, ИКР- иная контактная работа.

2.3 Содержание разделов дисциплины:

Раздел 1. Основные модели электронной коммерции. Угрозы безопасности электронной коммерции и электронных платежей.

Основные понятия и термины электронной коммерции и бизнеса. Понятие электронной коммерции.Краткий обзор основных понятий.Типология электронной коммерции.

Формирование способности решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; использование современных стандартов и методик, разработка регламентов для организации управления процессами жизненного цикла ИТ-инфраструктуры предприятий; организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия; умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия.

Раздел 2. Политика информационной безопасности. Построение систем безопасности электронного бизнеса.

Потенциальные угрозы электронного бизнеса. Основные задачи обеспечения безопасности информации хозяйствующего субъекта при ведении электронного бизнеса.

Оценка уязвимости систем электронной коммерции.Анализ и механизмы оценки рисков электронного бизнеса.Построение модели злоумышленника.Классификация преступлений в электронном бизнесе.Классификация и общая характеристика компьютерных преступлений.Анализ и оценка последствий компьютерных преступлений на основе современной статистики.

Формирование способности решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; использование современных стандартов и методик, разработка регламентов для организации управления процессами жизненного цикла ИТ-инфраструктуры предприятий; организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия; умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия.

Раздел 3. Методы и средства обеспечения информационной безопасности электронного бизнеса

Политика информационной безопасности в системах электронной коммерции. Стандарты построения систем защиты информации и практическое применение их требований для обеспечения информационной безопасности систем электронной коммерции. Корпоративные стандарты обеспечения информационной безопасности систем. Стандарт Центрального банка России по защите информации (СТО БР ИББС-3.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (с изменениями 2014 г.). Основы построения и менеджмента систем безопасности электронного бизнеса. Аудит систем информационной безопасности электронного бизнеса.

Формирование способности решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; использование современных стандартов и методик, разработка регламентов для организации управления процессами жизненного цикла ИТ-инфраструктуры предприятий; организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия; умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия.

Раздел 4. Корпорат ивные стандарты обеспечения информационной безопасности систем.

Распределение функций и порядок взаимодействия подразделений на различных этапах жизненного цикла информационных подсистем. Ответственные за информационную безопасность в подразделениях. Администраторы штатных и дополнительных средств защиты. Подразделения технической защиты информации. Система организационно-распорядительных документов организации по вопросам обеспечения безопасности информационных технологий. Регламентация действий всех категорий сотрудников, допущенных к работе с информационными системами

Формирование способности решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; использование современных стандартов и методик, разработка регламентов для организации управления процессами жизненного цикла ИТ-инфраструктуры предприятий; организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия; умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия.

Раздел 5. Развитие информационно-коммуникационных технологий

Предпосылки быстрого развития информационно-коммуникационных технологий. Этапы развития информационно-коммуникационных технологий. Тенденции развития информационно-коммуникационных технологий. Развитие информационно-коммуникационных технологий и организационные изменения на предприятиях.

Формирование способности решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; использование современных стандартов и методик, разработка регламентов для организации управления процессами жизненного цикла ИТ-инфраструктуры предприятий; организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия; умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия.

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Основные модели электронной коммерции. Угрозы безопасности электронной коммерции и электронных платежей.	Основные понятия и термины электронной коммерции и бизнеса. Понятие электронной коммерции.Краткий обзор основных понятий.Типология электронной коммерции.	написание реферата, подготовка сообщений, презентаций
2	Политика информационной безопасности. Построение систем безопасности электронного бизнеса.	Потенциальные угрозы электронного бизнеса. Основные задачи обеспечения безопасности информации хозяйствующего субъекта при ведении электронного бизнеса. Оценка уязвимости систем электронной коммерции.Анализ и механизмы оценки рисков электронного бизнеса. Построение модели злоумышленника.Классификация преступлений в электронном бизнесе. Анализ и оценка последствий компьютерных преступлений на основе современной статистики.	написание реферата, подготовка сообщений, презентаций
3	Методы и средства обеспечения информационной безопасности электронного бизнеса	Политика информационной безопасности в системах электронной коммерции. Стандарты построения систем защиты информации и практическое применение их требований для обеспечения информационной безопасности систем электронной коммерции. Корпоративные стандарты обеспечения информационной безопасности систем. Основы построения и менеджмента систем безопасности электронного бизнеса.	написание реферата, подготовка сообщений, презентаций

4	Корпорат ивные стандарты обеспечения информационной безопасности систем.	Распределение функций и порядок взаимодействия подразделений на различных этапах жизненного цикла информационных подсистем. Ответственные за информационную безопасность в подразделениях. Администраторы штатных и дополнительных средств защиты. Подразделения технической защиты информации. Система организационно-распорядительных документов организации по вопросам обеспечения безопасности информационных технологий.	написание реферата, подготовка сообщений, презентаций
5	Развитие информационно-коммуникационных технологий	Современные технологии создания информационного продукта. Проектирование информационных модулей: понятие информационных модулей, классификация, структура, характеристики. Аналитико-синтетические способы обработки информации. Комплексная оценка качества информационных продуктов и услуг. Экономическая эффективность информационного бизнеса. Оценка конкурентоспособности информационного продукта и информационной услуги: показатели, методика оценки.	написание реферата, подготовка сообщений, презентаций

2.3.2 Занятия практического типа.

№	Наименование раздела	Тематика практических занятий	Форма текущего контроля
1	2	3	4
1.	Основные модели электронной коммерции. Угрозы безопасности электронной коммерции и электронных платежей.	Структура основных бизнес-моделей электронной коммерции. Основные отличия и особенности моделей. Построение модели злоумышленника.Классификация преступлений в электронном бизнесе.	Устный опрос
2.	Политика информационной безопасности. Построение систем безопасности электронного	Сетевые угрозы, уязвимости и атаки.Средства обнаружения уязвимостей узлов IP-сетей и атак на узлы, протоколы и сетевые службы. Получение оперативной информации о новых уязвимостях и атаках.Способы устранения уязвимостей и противодействия вторжениям нарушителей.	Устный опрос

	бизнеса.		
3.	Методы и средства обеспечения информационной безопасности электронного бизнеса	Классификация и общая характеристика компьютерных преступлений. Анализ и оценка последствий компьютерных преступлений на основе современной статистики.	Устный опрос
4.	Корпоративные стандарты обеспечения информационной безопасности систем.	Распределение функций и порядок взаимодействия подразделений на различных этапах жизненного цикла информационных подсистем. Ответственные за информационную безопасность в подразделениях. Администраторы штатных и дополнительных средств защиты. Подразделения технической защиты информации.	Устный опрос
5.	Развитие информационно-коммуникационных технологий	Технология разработки метаинформативного и проблемноориентированного информационного модуля. Комплексная оценка качества информационных продуктов и услуг. Оценка структуры и содержания информационной услуги. Методы оценки качества информационного продукта. Экономическая эффективность информационного бизнеса.	Устный опрос

Примерный перечень тем рефератов, докладов, эссе

1. Субъекты информационных отношений, их интересы и безопасность, пути нанесения им ущерба.
2. Основные термины и определения.
3. Основные источники и пути реализации угроз.
1. Модели нарушителей.
2. Состав и организационная структура системы обеспечения информационной безопасности
3. Основные защитные механизмы.
4. Российские, зарубежные (британский BS7799 - ISO 17799 и германский BSI).
5. Международные стандарты и критерии защищенности систем (ISO15408-99).
6. Средства выявления уязвимостей узлов сетей и средства обнаружения атак на узлы, протоколы и сетевые службы.
7. Правовые и организационные вопросы обеспечения информационной безопасности и сохранности коммерческой тайны
8. Безопасность платежей в сети Интернет с использованием пластиковых карт.
9. Организационно-правовые вопросы защиты информации
10. Основные угрозы информационной безопасности и технические методы защиты.
11. Утечка по побочным каналам.
12. Защита информации в электронных платѐжных системах.
13. Электронная цифровая подпись. Назначение и использование.
14. Шифрование как средство защиты информации.

2.3.3 Лабораторные занятия

Лабораторные занятия - не предусмотрены

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

Таблица – Методическое обеспечение самостоятельной работы.

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Разбор теоретического материала по пособиям, конспектам лекций или видеолекциям;	1. «Положение о самостоятельной работе студентов»- Утвержденное 11.02.2011г. ФГБОУ ВО «КубГУ». 2. Гришина, Наталия Васильевна. Информационная безопасность предприятия [Текст] : учебное пособие для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность" / Н. В. Гришина. - 2-е изд., доп. - Москва : ФОРУМ : ИНФРА-М, 2015. - 238 с. - (Высшее образование. Бакалавриат). - Библиогр.: с. 200-204. - ISBN 978-5-00091-007-8. - ISBN 978-5-16-010494-2 3. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2017. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. АБС.URL https://www.biblio-online.ru/viewer/836C32FD-678E-4B11-8BFC-F16354A8AFC7#page/1 4. 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. АБС. URL https://www.biblio-online.ru/viewer/73BEF88E-FC6D-494A-821C-D213E1A984E1#page/1
2	Самостоятельное изучение указанных теоретических вопросов;	1. «Положение о самостоятельной работе студентов»- Утвержденное 11.02.2011г. ФГБОУ ВО «КубГУ». 2. Гришина, Наталия Васильевна. Информационная безопасность предприятия [Текст] : учебное пособие для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность" / Н. В. Гришина. - 2-е изд., доп. - Москва : ФОРУМ : ИНФРА-М, 2015. - 238 с. - (Высшее образование. Бакалавриат). -

		Библиогр.: с. 200-204. - ISBN 978-5-00091-007-8. - ISBN 978-5-16-010494-2 3. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2017. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. АБС.URL https://www.biblio-online.ru/viewer/836C32FD-678E-4B11-8BFC-F16354A8AFC7#page/1 4. 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. АБС. URL https://www.biblio-online.ru/viewer/73BEF88E-FC6D-494A-821C-D213E1A984E1#page/1
3	Подготовка рефератов	1. «Положение о самостоятельной работе студентов»- Утвержденное 11.02.2011г. ФГБОУ ВО «КубГУ». 2. Гришина, Наталия Васильевна. Информационная безопасность предприятия [Текст] : учебное пособие для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность" / Н. В. Гришина. - 2-е изд., доп. - Москва : ФОРУМ : ИНФРА-М, 2015. - 238 с. - (Высшее образование. Бакалавриат). - Библиогр.: с. 200-204. - ISBN 978-5-00091-007-8. - ISBN 978-5-16-010494-2 3. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2017. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. АБС.URL https://www.biblio-online.ru/viewer/836C32FD-678E-4B11-8BFC-F16354A8AFC7#page/1 4. 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. АБС. URL https://www.biblio-online.ru/viewer/73BEF88E-FC6D-494A-821C-D213E1A984E1#page/1
4	Подготовка выступлений на круглом столе	1. «Положение о самостоятельной работе студентов»- Утвержденное 11.02.2011г. ФГБОУ ВО «КубГУ». 2. Гришина, Наталия Васильевна. Информационная безопасность предприятия [Текст] : учебное пособие для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность" / Н. В. Гришина. - 2-е изд., доп. - Москва : ФОРУМ : ИНФРА-М, 2015.

		- 238 с. - (Высшее образование. Бакалавриат). - Библиогр.: с. 200-204. - ISBN 978-5-00091-007-8. - ISBN 978-5-16-010494-2 3. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2017. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. АБС.URL https://www.biblio-online.ru/viewer/836C32FD-678E-4B11-8BFC-F16354A8AFC7#page/1 4. 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. АБС. URL https://www.biblio-online.ru/viewer/73BEF88E-FC6D-494A-821C-D213E1A984E1#page/1
5	подготовка к зачету	1. «Положение о самостоятельной работе студентов»- Утвержденное 11.02.2011г. ФГБОУ ВО «КубГУ». 2. Гришина, Наталия Васильевна. Информационная безопасность предприятия [Текст] : учебное пособие для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность" / Н. В. Гришина. - 2-е изд., доп. - Москва : ФОРУМ : ИНФРА-М, 2015. - 238 с. - (Высшее образование. Бакалавриат). - Библиогр.: с. 200-204. - ISBN 978-5-00091-007-8. - ISBN 978-5-16-010494-2 3. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2017. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. АБС.URL https://www.biblio-online.ru/viewer/836C32FD-678E-4B11-8BFC-F16354A8AFC7#page/1 4. 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. АБС. URL https://www.biblio-online.ru/viewer/73BEF88E-FC6D-494A-821C-D213E1A984E1#page/1

Примеры вопросов для самостоятельной работы обучающихся

1. Основные понятия и термины электронной коммерции и бизнеса.
2. Структура основных бизнес-моделей электронной коммерции.
3. Платежные системы. Назначение и функции в экономике.
4. Виды электронной коммерции. Описание и характеристика.
5. Потенциальные угрозы электронного бизнеса.

6. Оценка уязвимости и рисков электронного бизнеса.
7. Направления обеспечения банковской безопасности.
8. Законодательство в области информационной безопасности.
9. Основные задачи обеспечения безопасности информации фирмы.
10. Классификация преступлений в электронном бизнесе.
11. Оценка последствий компьютерных преступлений (примеры).
12. Политика информационной безопасности. Основные положения.
13. Программные методы зашиты информации.Перечень и характеристика.
14. Технические методы защиты информации.
15. Безопасность электронной коммерции в Internet.
16. Антивирусная защита. Алгоритм работы антивирусной программы.
17. Аппаратный и программный брандмауэр. Назначение и алгоритм работы.
Методы и средства защиты информации при работе с электронной почтой.

3. Образовательные технологии.

С точки зрения применяемых методов используются как традиционные информационно-объяснительные лекции, так и интерактивная подача материала с мультимедийной системой. Компьютерные технологии в данном случае обеспечивают возможность разнопланового отображения алгоритмов и демонстрационного материала. Такое сочетание позволяет оптимально использовать отведенное время и раскрывать логику и содержание дисциплины.

Лекции представляют собой систематические обзоры основных аспектов дисциплины.

Практические занятия проводятся в компьютерных классах, при этом практикуется работа в группах. Подход разбора конкретных ситуаций широко используется как преподавателем, так и студентами при проведении анализа результатов самостоятельной работы. Это обусловлено тем, что в процессе исследования часто встречаются задачи, для которых единых подходов не существует. Каждая конкретная задача при своем исследовании имеет множество подходов, а это требует разбора и оценки целой совокупности конкретных ситуаций.

При освоении дисциплины используются следующие сочетания видов учебной работы с методами и формами активизации познавательной деятельности бакалавров для достижения запланированных результатов обучения и формирования компетенций.

Таблица - Сочетание видов ОД с различными методами ее активизации для очной формы обучения.

Вид занятия	Используемые интерактивные образовательные технологии	Количество часов
Практические	Групповая дискуссия.	2
Лекция	Проблемная лекция	2

Лекция	Лекция – визуализация	-
	ИТОГО	4

В процессе проведения занятий применяются интерактивные методы обучения.

Групповая дискуссия. Это метод организации совместной коллективной деятельности, позволяющий в процессе непосредственного общения путем логических доводов воздействовать на мнения, позиции и установки участников дискуссии. Целью дискуссии является интенсивное и продуктивное решение групповой задачи. Метод групповой дискуссии обеспечивает глубокую проработку имеющейся информации, возможность высказывания студентами разных точек зрения по заданной преподавателем проблеме, тем самым способствуя выработке адекватного в данной ситуации решения. Метод групповой дискуссии увеличивает вовлеченность участников в процесс этого решения, что повышает вероятность его реализации.

Проблемная лекция - на этой лекции новое знание вводится через проблемность вопроса, задачи или ситуации. При этом процесс познания студентов в сотрудничестве и диалоге с преподавателем приближается к исследовательской деятельности. Содержание проблемы раскрывается путем организации поиска ее решения или суммирования и анализа традиционных и современных точек зрения.

Проблемная лекция начинается с вопросов, с постановки проблемы, которую в ходе изложения материала необходимо решить. Проблемные вопросы отличаются от не проблемных тем, что скрытая в них проблема требует не однотипного решения, то есть, готовой схемы решения в прошлом опыте нет. Лекция строится таким образом, чтобы обусловить появление вопроса в сознании студента. Учебный материал представляется в форме учебной проблемы. Она имеет логическую форму познавательной задачи, отмечающей некоторые противоречия в ее условиях и завершающейся вопросами, которые это противоречие объективирует. Проблемная ситуация возникает после обнаружения противоречий в исходных данных учебной проблемы. Для проблемного изложения отбираются важнейшие разделы курса, которые составляют основное концептуальное содержание учебной дисциплины, являются наиболее важными для профессиональной деятельности и наиболее сложными для усвоения слушателей. Учебные проблемы должны быть доступными по своей трудности для слушателей.

Лекция – визуализация. Данный вид лекции является результатом нового использования принципа наглядности. Подготовка данной лекции преподавателем состоит в том, чтобы изменить, переконструировать учебную информацию по теме лекционного занятия в визуальную форму для представления студентам через технические средства обучения или вручную (схемы, рисунки, чертежи и т.п.). Чтение лекции сводится к связному, развернутому комментированию преподавателем подготовленных наглядных материалов, полностью раскрывающему тему данной лекции. Лучше всего использовать разные виды визуализации - натуральные, изобразительные, символические, - каждый из которых или их сочетание выбирается в зависимости от содержания учебного материала. Этот вид лекции лучше всего использовать на этапе введения слушателей в новый раздел, тему, дисциплину.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

4.1 Фонд оценочных средств для проведения текущего контроля.

1. Архитектура системы защиты конфиденциального документооборота на предприятии.
2. Основные направления формирования конфиденциальных документов на предприятии.
3. Предпосылки отнесения информации к категории конфиденциальной и выявление конфиденциальных сведений на предприятии.
4. Порядок документирования конфиденциальных сведений.
5. Основные носители конфиденциальных сведений и угрозы конфиденциальному документообороту.
6. Жизненный цикл конфиденциального документа.
7. Структура документированной системы защиты в РФ.
8. Цели и задачи Политики информационной безопасности на предприятии
9. Уровни Политики информационной безопасности на предприятии.
10. Разработка Концепции безопасности информации и Регламента обеспечения безопасности информации на предприятии.
11. Понятие Профиль защиты и его составляющие.
12. Система физической защиты (СФЗ): основные задачи и способы их решения на предприятии.
13. Сценарии последовательности действий нарушителя СФЗ.
14. Организация инженерно-технических средств охраны.
15. Международные стандарты в области информационной безопасности.
16. Цели, задачи и стадии проведения аудита информационной безопасности.
17. Виды аудита информационной безопасности, применяемые на различных стадиях жизненного цикла обследуемого объекта.
18. Состав работ по проведения аудита информационной безопасности.

Вопросы для проведения текущего контроля

4.2 Фонд оценочных средств для проведения промежуточной аттестации

Вопросы для подготовки к экзамену

1. Основные типы электронной коммерции: Интернет-коммерция, мобильная коммерция, телевизионная коммерция. Общие и отличительные черты электронной коммерции и Интернет-коммерции.
2. Стандарты классификации товаров и услуг. Стандарты UN/EDIFACT и технология XML. Мобильные средства ведения электронного бизнеса.
3. Характеристики сети Интернет как информационно-технологической среды электронной коммерции.
4. Стратегии развития электронных торговых площадок.
5. Особенности и перспективы развития электронных торговых площадок в РФ.
6. Организация размещения государственных и муниципальных заказов на электронных торговых площадках.
7. Информационные риски предприятий электронного бизнеса.
8. Информационная безопасность и защита информации в сфере электронного бизнеса.
9. Стандарты менеджмента информационной безопасности серии 27000. Критерии оценки безопасности информационных технологий.

10. Основные уязвимости программного обеспечения. Классификация уязвимостей и атак.

11. Основные методы защиты уязвимостей программного обеспечения.

12. Утечка конфиденциальной информации. Способы защиты. Системы предотвращения Утечка конфиденциальной информации. Политика безопасности организации в области предотвращения утечки информации.

13. Защита информации и информационная безопасность в сфере электронного бизнеса. ГОСТ Р

14. ИСО/МЭК «Критерии оценки безопасности информационных технологий - 15408».

15. Стандарты менеджмента информационной безопасности серии 27000.

16. Определение DoS атаки.Виды DDoS атак. Методы определения DoS атаки. Способ борьбы с атаками на отказ в обслуживании DDoS. Стресс-тестирование и DoS атаки.

17. Социальная инженерия. Определения, методы и схемы. Защита от социальной инженерии.

18. Защита корпоративной системы безопасности.

19. Виды систем оплаты в Интернет. Российские платежные системы. Сравнение технологий оплаты и уровня их безопасности. Защита электронных платежных систем.

20. Основные протоколы взаимодействия. Протокол SET. Протокол SSL. Сравнительные характеристики протоколов SSL и SET.

21. Электронная подпись. Использование электронной подписи в электронном бизнесе.

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 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.

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

5.1 Основная литература:

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2017. — 321 с. — (Серия : Университеты России). —URL :https://www.biblio-online.ru/viewer/836C32FD-678E-4B11-8BFC-F16354A8AFC7#page/1
2. 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). —URL: https://www.biblio-online.ru/viewer/73BEF88E-FC6D-494A-821C-D213E1A984E1#page/1

5. 2. Дополнительная литература:

1. Баранова, Елена Константиновна. Информационная безопасность и защита информации [Текст] : учебное пособие для студентов, обучающихся по направлению "Прикладная информатика" / Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - Москва : РИОР : ИНФРА-М, 2016. - 321 с. - (Высшее образование). - Библиогр.: с. 313-316. - ISBN 978-5-369-01450-9. - ISBN 978-5-16-011164-3
2. Гришина, Наталия Васильевна. Информационная безопасность предприятия [Текст] : учебное пособие для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность" / Н. В. Гришина. - 2-е изд., доп. - Москва : ФОРУМ : ИНФРА-М, 2015. - 238 с. - (Высшее образование. Бакалавриат). - Библиогр.: с. 200-204. - ISBN 978-5-00091-007-8. - ISBN 978-5-16-010494-2
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М. : Издательство Юрайт, 2017. — 312 с. — (Серия : Специалист). — .URL: https://www.biblio-online.ru/viewer/E458AFCD-826E-4A1F-9BAB-68BB83EA616F#page/1
4. Современные информационно-коммуникационные технологии для успешного ведения бизнеса [Текст] : учебное пособие / [Ю. Д. Романова и др.]. - Москва : ИНФРА-М, 2014. - 178 с
5. Информационные системы и технологии управления [Текст] : учебник для студентов вузов / под ред. Г. А. Титоренко. - 3-е изд., перераб. и доп. - М. : ЮНИТИ-ДАНА, 2010. - 591 с.

5.3. Периодические издания:

1. “Финансовый менеджмент”/Научный журнал/Периодичность – 6 раз в год/ сайт: https://elibrary.ru/title_about.asp?id=9552
2. “Алгебра и логика” / Институт математики им.Соболева СО РАН /Периодичность – 6 раз в год/ сайт: http://elibrary.ru/title_about.asp?id=7311/

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

1. Российское образование, федеральный портал [Официальный сайт] — URL: http://www.edu.ru
2. Образовательный портал «Учеба» [Официальный сайт] URL: http://www.ucheba.com/

3. Портал «Российское образование» [Официальный сайт] URL: http://www.edu.ru/

4. Единое окно доступа к образовательным ресурсам «Единое окно» [Официальный сайт] URL: http://window.edu.ru/

5. Федеральная университетская компьютерная сеть России [Официальный сайт] URL: http://www.runnet.ru/

6. Служба тематических толковых словарей[Официальный сайт] URL: http://www.glossary.ru/

7. Образовательный портал [Официальный сайт] URL: «Академик» http://dic.academic.ru/

8. Web of Sciense (архив с 2002 года) рефераты [Официальный сайт] URL: http://webofknowledge.com.

9. Лекториум "(Минобрнауки РФ) единая Интернет-библиотека лекций [Официальный сайт] URL http://www.lektorium.tv/

10. Электронный архив документов КубГУ полнотекстов [Официальный сайт] URL: http://docspace.kubsu.ru

7. Методические указания для обучающихся по освоению дисциплины.

Согласно письма Министерства образования и науки РФ № МОН-25486 от 21.06.2017г «О разработке адаптированных образовательных программ» -Разработка адаптивной программы необходима в случае наличия в образовательной организации хотя бы одного обучающегося с ограниченными возможностями здоровья.

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.

Система обучения основывается на рациональном сочетании нескольких видов учебных занятий (в первую очередь, лекций и практических (лабораторных) занятий), работа на которых обладает определенной спецификой.

Подготовка к лекциям.

Знакомство с дисциплиной происходит уже на первой лекции, где от требуется не просто внимание, но и самостоятельное оформление конспекта. Конспектирование лекций – сложный вид аудиторной работы, предполагающий интенсивную умственную деятельность студента. Конспект является полезным тогда, когда записано самое существенное. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Целесообразно вначале понять основную мысль, излагаемую лектором, а затем записать ее. Желательно запись осуществлять на одной странице листа или оставляя поля, на которых позднее, при самостоятельной работе с конспектом, можно сделать дополнительные записи, отметить непонятные места.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, предложенные преподавателям. Следует обращать внимание на акценты, выводы, которые делает лектор, отмечая наиболее важные моменты в лекционном материале замечаниями «важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Работая над конспектом лекций, Вам всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

Подготовка к практическим занятиям.

Подготовку к каждому практическому занятию необходимо начать с ознакомления с планом практического занятия, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, рекомендованной к данной теме. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Подготовка к лабораторным занятиям и практикумам носит различный характер, как по содержанию, так и по сложности исполнения. Проведение прямых и косвенных измерений предполагает детальное знание измерительных приборов, их возможностей, умение вносить своевременные поправки для получения более точных результатов . Многие лабораторные занятия требуют большой исследовательской работы, изучения дополнительной научной литературы.

В процессе подготовки к практическим занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы. При всей полноте конспектирования лекции в ней невозможно изложить весь материал. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала.

Защита лабораторных работ должна происходить, как правило, в часы, отведенные на лабораторные занятия. Студент может быть допущен к следующей лабораторной работе только в том случае, если у него не защищено не более двух предыдущих работ.

Рекомендации по работе с литературой.

Работу с литературой целесообразно начать с изучения общих работ по теме, а также учебников и учебных пособий. Далее рекомендуется перейти к анализу монографий и статей, рассматривающих отдельные аспекты проблем, изучаемых в рамках курса, а также официальных материалов и неопубликованных документов (научно-исследовательские работы, диссертации), в которых могут содержаться основные вопросы изучаемой проблемы.

Работу с источниками надо начинать с ознакомительного чтения, т.е. просмотреть текст, выделяя его структурные единицы. При ознакомительном чтении закладками отмечаются те страницы, которые требуют более внимательного изучения.

В зависимости от результатов ознакомительного чтения выбирается дальнейший способ работы с источником. Если для разрешения поставленной задачи требуется изучение некоторых фрагментов текста, то используется метод выборочного чтения. Если в книге нет подробного оглавления, следует обратить внимание обучающихся на предметные и именные указатели.

Избранные фрагменты или весь текст (если он целиком имеет отношение к теме) требуют вдумчивого, неторопливого чтения с «мысленной проработкой» материала. Такое чтение предполагает выделение: 1) главного в тексте; 2) основных аргументов; 3) выводов. Особое внимание следует обратить на то, вытекает тезис из аргументов или нет.

Необходимо также проанализировать, какие из утверждений автора носят проблематичный, гипотетический характер, и уловить скрытые вопросы.

Понятно, что умение таким образом работать с текстом приходит далеко не сразу. Наилучший способ научиться выделять главное в тексте, улавливать проблематичный характер утверждений, давать оценку авторской позиции – это сравнительное чтение, в ходе которого Вы знакомитесь с различными мнениями по одному и тому же вопросу, сравниваете весомость и доказательность аргументов сторон и делаете вывод о наибольшей убедительности той или иной позиции.

При наличии расхождений между авторами необходимо найти рациональное зерно у каждого из них, что позволит глубже усвоить предмет изучения и более критично оценивать изучаемые вопросы. Знакомясь с особыми позициями авторов, нужно определять их схожие суждения, аргументы, выводы, а затем сравнивать их между собой и применять из них ту, которая более убедительна.

Следующим этапом работы с литературными источниками является создание конспектов, фиксирующих основные тезисы и аргументы..

Таким образом, при работе с источниками и литературой важно уметь:

- сопоставлять, сравнивать, классифицировать, группировать, систематизировать информацию в соответствии с определенной учебной задачей;
- обобщать полученную информацию, оценивать прослушанное и прочитанное;
- фиксировать основное содержание сообщений; формулировать, устно и письменно, основную идею сообщения; составлять план, формулировать тезисы;
- готовить и презентовать развернутые сообщения типа доклада;
- работать в разных режимах (индивидуально, в паре, в группе), взаимодействуя друг с другом;
- пользоваться реферативными и справочными материалами;
- контролировать свои действия и действия своих товарищей, объективно оценивать свои действия;
- обращаться за помощью, дополнительными разъяснениями к преподавателю, другим студентам;
- пользоваться лингвистической или контекстуальной догадкой, словарями различного характера, различного рода подсказками, опорами в тексте (ключевые слова, структура текста, предваряющая информация и др.);
- использовать при говорении и письме перифраз, синонимичные средства, слова-описания общих понятий, разъяснения, примеры, толкования, «словотворчество»;
- повторять или перефразировать реплику собеседника в подтверждении понимания его высказывания или вопроса;
- обратиться за помощью к собеседнику (уточнить вопрос, переспросить и др.);

Подготовка к промежуточной аттестации.

При подготовке к промежуточной аттестации целесообразно:

- внимательно изучить перечень вопросов и определить, в каких источниках находятся сведения, необходимые для ответа на них;
- внимательно прочитать рекомендованную литературу;
- составить краткие конспекты ответов (планы ответов).

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

8.1 Перечень информационных технологий.

– Проверка домашних заданий и консультирование посредством электронной почты.

– Использование электронных презентаций при проведении практических занятий.

8.2 Перечень необходимого программного обеспечения.

№	Перечень лицензионного программного обеспечения
1	WinRAR, Государственный контракт №13-ОК/2008-3
2	Microsoft Windows XP, Государственный контракт №13-ОК/2008-3
3	Microsoft Windows Server Std 2003, Государственный контракт №13-ОК/2008-2 (Номер лицензии - 43725353)
4	Microsoft Windows Office 2003 Pro, Государственный контракт №13-ОК/2008-3 (Номер лицензии - 43725353)

8.3 Перечень информационных справочных систем:

1. Федеральная служба государственной статистики: www.gks.ru
2. Информационный портал Всемирного банка: http//data.worldbank.org.
3. Эконометрический пакет Eviews http://www.eviews.com/home.html
4. Eviews http://statmethods.ru/trainings/eviews.html

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

№	Наименование специальных помещений и помещений для самостоятельной работы	Номера аудиторий / кабинетов
1.	учебные аудитории для проведения занятий лекционного типа	501,502,503,505,506,507,508, 509, 510,513,514
2.	учебные аудитории для проведения занятий семинарского типа	501,502,503,505,506,507,508, 509, 510,513,514
3.	Компьютерные классы с выходом в Интернет	503,509,510
4.	учебные аудитории для выполнения научно – исследовательской работы (курсового проектирования)	Кабинет курсового проектирования (выполнения курсовых работ) - № 503, 509, 510 Оборудование: мультимедийный проектор, экран, персональные компьютеры, учебная мебель, доска учебная, выход в Интернет, учебно-наглядные пособия (тематические иллюстрации), презентации на электронном носителе, сплит-система
5.	учебные аудитории для самостоятельной работы, с рабочими местами, оснащенными компьютерной техникой с подключением к сети	Кабинет для самостоятельной работы - № 504,509,510 Оборудование: персональные компьютеры, учебная мебель, доска учебная, выход в Интернет

	«Интернет» и обеспечением неограниченного доступа в электронную информационно-образовательную среду организации для каждого обучающегося, в соответствии с объемом изучаемых дисциплин	
6.	Исследовательские лаборатории (центров), оснащенные лабораторным оборудованием	Компьютерный класс № 510 : мультимедийный проектор, экран, персональные компьютеры, учебная мебель, доска учебная, выход в Интернет, наглядные пособия. Сетевое оборудование CISCO (маршрутизаторы, коммутаторы, 19-ти дюймовый сетевой шкаф) сплит-система, стенд «Архитектура ПЭВМ»
7.	учебные аудитории групповых и индивидуальных консультаций	№508 Оборудование: персональный компьютер, учебная мебель, доска учебная, учебно-наглядные пособия (тематические иллюстрации), сканер, доска магнитно-маркерная, стеллажи с учебной и периодической литературой
8.	Помещение для хранения и профилактического обслуживания учебного оборудования	Помещение № 511, Помещение № 516, Помещение № 517, Помещение № 518
9.	учебные аудитории для проведения текущей и промежуточной аттестации	501,502,503,505,506,507,508, 509, 510,513,514

Согласно письма Министерства образования и науки РФ № МОН-25486 от 21.06.2017г «О разработке адаптированных образовательных программ» -Разработка адаптивной программы необходима в случае наличия в образовательной организации хотя бы одного обучающегося с ограниченными возможностями здоровья

Для обучающихся из числа инвалидов обучение проводится организацией с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья (далее - индивидуальные особенности).

При проведении обучения инвалидов обеспечивается соблюдение следующих общих требований:

-проведение обучения для инвалидов в одной аудитории совместно с обучающимися, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для обучающихся;

-присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся инвалидам необходимую техническую помощь с учетом их индивидуальных особенностей;

-пользование необходимыми обучающимся инвалидам техническими средствами с учетом их индивидуальных особенностей;

-обеспечение возможности беспрепятственного доступа обучающихся инвалидов в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях;

В зависимости от индивидуальных особенностей обучающихся с ограниченными

возможностями здоровья, организация обеспечивает выполнение следующих требований при проведении занятий:

а) для слепых:

-задания и иные материалы оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом;

-письменные задания выполняются обучающимися на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых, либо надиктовываются ассистенту;

-при необходимости обучающимся предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

б) для слабовидящих:

-задания и иные материалы оформляются увеличенным шрифтом;

-обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

-при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

-обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования;

г) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

-письменные задания выполняются обучающимися на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

Обучающийся инвалид при поступлении подает письменное заявление о необходимости создания для него специальных условий при проведении обучения с указанием особенностей его психофизического развития, индивидуальных возможностей и состояния здоровья (далее - индивидуальные особенности). К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в организации).