



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 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.02 Информационная безопасность

Направление подготовки:	38.03.05 Бизнес-информатика
Направленность (профиль):	Электронный бизнес
Программа подготовки	академическая
Форма обучения	очная
Квалификация (степень) выпускника	бакалавр

Краснодар 2017

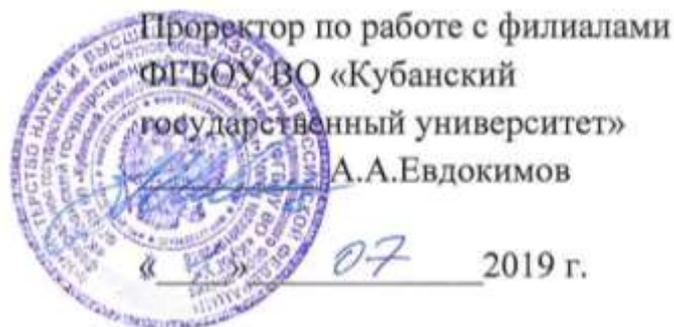


1920

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

филиал Федерального государственного бюджетного образовательного
учреждения высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
в г. Новороссийске
Кафедра информатики и математики

УТВЕРЖДАЮ



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.02 Информационная безопасность

Направление подготовки: 38.03.05 Бизнес-информатика

Направленность (профиль): Электронный бизнес

Программа подготовки: академическая

Форма обучения: очная

Квалификация (степень) выпускника: Бакалавр

Краснодар 2019

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

на рабочую программу учебной дисциплины
«Информационная безопасность»

для бакалавров 38.03.05 Бизнес-информатика
филиал ФГБОУ ВО «КубГУ» в г.Новороссийске

Рабочая учебная программа соответствует требованиям ФГОС ВО по направлению 38.03.05 Бизнес-информатика по предмету «Информационная безопасность». Все основные понятия предмета нашли свое отражение в перечне представленных в рабочей учебной программе необходимых знаний. Распределение времени, отводимого на изучение различных разделов, включая самостоятельную работу, соответствует их трудоемкости. Приведенные в рабочей учебной программе примеры заданий и итоговых вопросов позволяют определить уровень знаний и умений обучающихся.

Задания рабочей учебной программы подобраны логично. Последовательность тем, предлагаемых к изучению, направлена на качественное усвоение учебного материала. Лабораторные или практические задания разнообразны, позволяют адекватно оценивать уровень знаний обучающихся по предмету. Методические рекомендации по лабораторным или практическим занятиям обеспечивают формирование базовых умений для выполнения исследований в процессе научного познания и теоретического обоснования профессиональных задач.

Считаю, что указанная рабочая учебная программа может быть рекомендована для внедрения в учебный процесс при подготовке бакалавров по направлению 38.03.05 Бизнес-информатика.

Директор
ООО «Финам - Новороссийск»



А.Е. Адамович

ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ
на рабочую программу учебной дисциплины
«Информационная безопасность»
для бакалавров 38.03.05 Бизнес-информатика
филиал ФГБОУ ВО «КубГУ» в г.Новороссийске

Рабочая учебная программа дисциплины «Информационная безопасность» для бакалавров 38.03.05 Бизнес-информатика, содержит перечень формируемых компетенций и этапы их формирования; показатели, критерии оценки компетенций и типовые контрольные задания; материалы для аттестации обучающихся. Содержание рабочей учебной программы дисциплины «Информационная безопасность» соответствует ФГОС ВО по направлению подготовки 38.03.05 Бизнес-информатика и учебному плану.

Рабочая учебная программа соотносится с фондом оценочных средств. Его наполнение позволяет объективно оценить уровень усвоения материала обучающимися.

Программа имеет четкий компетентностный подход к решению поставленных задач.

В рецензируемой программе есть все необходимые разделы, составленные на соответствующем научном и методическом уровне. Практическая направленность данной программы не подлежит сомнению.

В рабочей программе указаны требования к результатам освоения дисциплины. Всё это позволяет обеспечивать приобретение обучающимися знаний, умений и навыков, направленных на формирование компетентностной модели обучающегося.

Рабочая программа составлена квалифицированно, демонстрирует профессионализм и высокий уровень методической подготовки и может быть использована в образовательном процессе

Директор по развитию
ООО «АЙТИ БИЗНЕС ЮГ»



М.К. Кунина.

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 30.08.2017г.



Заведующий кафедрой (разработчика) Рзун И.Г

Рабочая программа обсуждена на заседании кафедры информатики и математики протокол № 1 от 30.08.2017г.



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 30.08.2017г.

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
 - 1.2 Задачи дисциплины.
 - 1.3 Место дисциплины в структуре образовательной программы
 - 1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.
2. Структура и содержание дисциплины.
 - 2.1 Распределение трудоёмкости дисциплины по видам работ.
 - 2.2 Структура дисциплины
 - 2.3 Содержание разделов дисциплины
 - 2.3.1 Занятия лекционного типа.
 - 2.3.2 Занятия практического типа.
 - 2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине
3. Образовательные технологии.
4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.
 - 4.1 Фонд оценочных средств для проведения текущего контроля.
 - 4.2 Фонд оценочных средств для проведения промежуточной аттестации.
5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.
 - 5.1 Основная литература
 - 5.2 Дополнительная литература
 - 5.3. Периодические издания:
6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.
7. Методические указания для обучающихся по освоению дисциплины.
8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.
 - 8.1 Перечень информационных технологий.
 - 8.2 Перечень необходимого программного обеспечения.
 - 8.3 Перечень информационных справочных систем
9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.

1 Цели и задачи изучения дисциплины.

1.1 Цель освоения дисциплины.

Целью освоения учебной дисциплины Б1.В.02 «Информационная безопасность» является приобретение теоретических и практических умений и навыков применения современных информационных технологий для использования в профессиональной деятельности по защите информации.

1.2 Задачи дисциплины.

Задачами дисциплины являются:

- формирование у обучающихся общего представления о современных концепциях информационной безопасности;
- знакомство с различными методами защиты информации от несанкционированного доступа;
- изучение криптографических средств, как основного инструмента обеспечения сохранности компьютерной информации;
- подготовка отчетов, обзоров;
- поиск, сбор, обработка и систематизация информации об экономике и ИКТ;
- приобретение практических навыков работы с современными аппаратными и программными средствами защиты информации.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к вариативной части обязательных дисциплин учебного плана.

Данный курс наиболее тесно связан с курсами: «Развитие информационного общества», «Теоретические основы информатики», «Моделирование бизнес-процессов», «Вычислительные системы, сети, телекоммуникации» и является дальнейшим развитием прикладных аспектов названных дисциплин.

Компетенции, знания, навыки и умения, полученные в ходе изучения дисциплины, должны всесторонне использоваться и развиваться студентами:

- на всех этапах обучения в вузе при изучении различных дисциплин учебного плана: при разработке проектной документации, решении информационно-поисковых и учетно-аналитических задач, проведении научных исследований, оформлении результатов самостоятельной работы, выполнении контрольных домашних заданий, подготовке рефератов, эссе, докладов, курсовых и дипломных работ;
- в ходе дальнейшего обучения в магистратуре и аспирантуре;
- в процессе последующей профессиональной деятельности при решении прикладных задач, требующих знания средств электронно- вычислительной техники, формирования проектов необходимого программно-технического обеспечения вычислительных систем и коммуникаций для организации деятельности финансовых учреждений.

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

Процесс изучения дисциплины направлен на формирование следующих общепрофессиональных и профессиональных компетенций: ОПК-1, ПК-9, ПК-11.

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			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.	-определять набор требований по защите информации в текущих условиях. - учитывать тенденции развития техники	-навыком поиска необходимых РД. - навыками работы с Российской и зарубежной научно-исследовательской литературой.
2	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
3	ПК-11	умение защищать права на интеллектуальную собственность	Знать: -общие принципы правовой охраны и основные институты интеллектуальной собственности;	Уметь: -определять оптимальные способы защиты права интеллектуальной собственности	Владеть: -навыками защиты права интеллектуальной собственности

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 4 зач.ед. (108 часов), их распределение по видам работ представлено в таблице

Вид учебной работы	Всего часов	Семестры (часы)				
		5				
Контактная работа, в том числе:	55,3	55,3				
Аудиторные занятия (всего):	52	52				
Занятия лекционного типа	18	18		-	-	
Лабораторные занятия				-	-	
Занятия семинарского типа (семинары, практические занятия)	34	34		-	-	
	-	-		-	-	
Иная контактная работа:	3,3	3,3				
Контроль самостоятельной работы (КСР)	3	3				
Промежуточная аттестация (ИКР)	0,3	0,3				
Самостоятельная работа, в том числе:	17	17				
Курсовая работа	-	-		-	-	
Проработка учебного (теоретического) материала	10	10		-	-	
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)	5	5		-	-	
Реферат	2	2		-	-	
Подготовка к текущему контролю				-	-	
Контроль:						
Подготовка к экзамену	35,7	35,7				
Общая трудоемкость	час.	108	108		-	-
	в том числе контактная работа	55,3	55,3			
	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 5 семестре

№	Наименование разделов	Количество часов						
		Всего	Контактная работа				Контроль	Самостоятельная работа СР
			Л	ПЗ	ИКР	КСР		
1.	Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ	14	4	7				3
2.	Построение системы защиты информации в организации	13	3	7				3
3.	Современные методики анализа и управления рисками информационной безопасности	14	4	7				3
4	Криптографическая защита информации	14	3	7				4
5	Архитектура информационной безопасности предприятия	14	4	6				4
	Итого по дисциплине	69	18	34				17
	Промежуточная аттестация (ИКР)	0,3			0,3			
	КСР	3				3		
	Контроль	35,7					35,7	
	<i>Всего:</i>	108	18	34	0,3	3	35,7	17

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 Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ

Понятие информации. Фазы обращения информации в информационных системах. Место информационной безопасности в национальной безопасности РФ. Цели и задачи обеспечения информационной безопасности. Составляющие информационной безопасности. Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности. Виды и источники угроз информационной безопасности РФ. Структура государственной системы обеспечения информационной безопасности РФ.

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; организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия; умения защищать права на интеллектуальную собственность

Раздел 2. Построение системы защиты информации в организации

Архитектура СЗИ организации и основные требования к средствам защиты. Функциональное построение СЗИ организации и назначение основных подразделений. Элементарные модели СЗИ организации. Семирубежная модель защиты. Последовательность и содержание основных этапов проектирования СЗИ организации. Содержание процесса эксплуатации СЗИ организации. Анализ угроз информационной безопасности. Внутренние и внешние источники угроз информационной безопасности. Схема воздействия угроз на информационную систему. Перечень основных формальных и неформальных средств защиты информации. Стратегии защиты информации на объекте информатизации. Основы защиты информации в телекоммуникационных сетях. Роль персонала в обеспечении информационной безопасности предприятия.

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; организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия; умения защищать права на интеллектуальную собственность

Раздел 3. Современные методики анализа и управления рисками информационной безопасности

Управление рисками на различных стадиях жизненного цикла информационной системы. Трехмерная модель “куб безопасности”. Анализ информационных рисков, угроз и уязвимостей системы. Оценка рисков по двум факторам. Анализ информационных рисков, угроз и уязвимостей системы. Оценка рисков по трем факторам. Программное обеспечение для анализа рисков информационной безопасности.

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; организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия; умения защищать права на интеллектуальную собственность

Раздел 4. Криптографическая защита информации

Классические криптоалгоритмы – моно- и многоалфавитные подстановки. Классические криптоалгоритмы - перестановки. Шифрование методом гаммирования. Современные симметричные системы шифрования. Обобщенная схема симметричного шифрования. Симметричная система шифрования DES. Отечественный стандарт симметричного шифрования. Принцип открытого распространения ключей. Алгоритм Диффи-Хеллмана. Современные асимметричные системы шифрования. Обобщенная схема асимметричного шифрования. Асимметричная система шифрования RSA. Электронная цифровая подпись. Обобщенная схема постановки и проверки ЭЦП. Электронная цифровая подпись на основе алгоритма RSA. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2012.

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; организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия; умения защищать права на интеллектуальную собственность

Раздел 5. Архитектура информационной безопасности предприятия.

Задачи ИБ предприятия. Стратегическое выстраивание ИБ. Интеграция ИБ в бизнес-процессы. Принципы ИБ. Результативность ИБ. Интеграция компонентов ИБ. Архитектура информационной безопасности предприятия. Промышленная модель ИБ. «Дорожная карта» развития ИБ предприятия. Доверенные зоны. Инфраструктура ИБ.

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; организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия; умения защищать права на интеллектуальную собственность

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ	Понятия : информация, информационная безопасность. Цели и задачи обеспечения информационной безопасности. Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности.	написание реферата, подготовка сообщений, презентаций
2.	Построение системы защиты информации в организации	Архитектура СЗИ организации и основные требования к средствам защиты. Анализ и управление рисками в сфере информационной безопасности. Криптографическая защита информации	написание реферата, подготовка сообщений, презентаций
3.	Современные методики анализа и управления рисками информационной безопасности	Методы защиты информации при передаче в телекоммуникационных сетях. Вредоносное программное обеспечение и методы борьбы с ним. Возможности и особенности сетевых вредоносных программ.	написание реферата, подготовка сообщений, презентаций
4.	Криптографическая защита информации	Отечественный стандарт симметричного шифрования ГОСТ 28147-89. Электронная цифровая подпись. Обобщенная схема постановки и проверки ЭЦП. Отечественный стандарт цифровой подписи ГОСТ Р34.10-2012. Защищенный электронный документооборот. Особенности защиты мультимедийного контента в телекоммуникационных сетях.	написание реферата, подготовка сообщений, презентаций
5.	Архитектура информационной безопасности предприятия	Задачи ИБ предприятия. Стратегическое выстраивание ИБ. Интеграция ИБ в бизнес-процессы. Принципы ИБ. Результативность ИБ. Интеграция компонентов ИБ. Архитектура	написание реферата, подготовка сообщений,

		информационной безопасности предприятия. Промышленная модель ИБ. «Дорожная карта» развития ИБ предприятия. Доверенные зоны. Инфраструктура ИБ.	презентаций
--	--	--	-------------

2.3.2 Занятия практического типа.

№	Наименование раздела	Тематика практических занятий	Форма текущего контроля
1	2	3	4
1.	Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ	Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности.	Устный опрос
2.	Построение системы защиты информации в организации	Архитектура СЗИ организации и основные требования к средствам защиты. Анализ и управление рисками в сфере информационной безопасности.	Устный опрос
3.	Современные методики анализа и управления рисками информационной безопасности	Вредоносное программное обеспечение и методы борьбы с ним. Возможности и особенности сетевых вредоносных программ. Методы защиты информации при передаче в телекоммуникационных сетях.	Устный опрос
4.	Криптографическая защита информации	Отечественный стандарт симметричного шифрования ГОСТ 28147-89. Электронная цифровая подпись. Обобщенная схема постановки и проверки ЭЦП. Отечественный стандарт цифровой подписи ГОСТ Р34.10-2012.	Устный опрос
5.	Архитектура информационной безопасности предприятия	Задачи ИБ предприятия. Интеграция ИБ в бизнес-процессы. Принципы ИБ... Архитектура информационной безопасности предприятия. Промышленная модель ИБ. Инфраструктура ИБ.	Устный опрос

Примерный перечень тем рефератов, докладов, эссе

1. Основные понятия информационной безопасности. Цель защиты информации в частном
2. и государственном секторе.
3. Современные требования к системе информационной безопасности организации.
4. Основные этапы создания системы защиты информации в организации.
5. Функциональное построение системы защиты информации.
6. Организационное построение системы защиты информации в организации.
7. Семирубежная модель защиты.
8. Практические проблемы обеспечения информационной безопасности.
9. Место информационной безопасности в системе национальной безопасности Российской Федерации.
10. Структура Государственной системы обеспечения информационной безопасности Российской Федерации.
11. Структура и задачи Федеральной службы по техническому и экспортному контролю, и ее роль в управлении информационной безопасностью в РФ.
12. Иерархия законодательства Российской Федерации в области информационной безопасности.
13. ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ от 9 сентября 2000 г. № Пр-1895.
14. ФЕДЕРАЛЬНЫЙ ЗАКОН ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ от 27 июля 2006 года N 149-ФЗ.
15. Федеральный закон Российской Федерации "Об электронной подписи" от 6 апреля 2011 г. N 63-ФЗ.
16. Федеральный закон Российской Федерации "О персональных данных" от 27 июля 2006 г. N 152-ФЗ.
17. Основные направления обеспечения информационной безопасности на предприятии.
18. Многоуровневая структура системы защиты информации на предприятии.
19. Стратегии организации защиты информации на предприятии.
20. Архитектура системы защиты конфиденциального документооборота на предприятии.
21. Основные направления формирования конфиденциальных документов на предприятии.
22. Предпосылки отнесения информации к категории конфиденциальной и выявление конфиденциальных сведений на предприятии.
23. Порядок документирования конфиденциальных сведений.
24. Основные носители конфиденциальных сведений и угрозы конфиденциальному документообороту.
25. Жизненный цикл конфиденциального документа.
26. Структура документированной системы защиты в РФ.

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;	<ol style="list-style-type: none"> 1. «Положение о самостоятельной работе студентов»- Утвержденное 11.02.2011г. ФГБОУ ВО «КубГУ». 2. Баранова, Е. К. Информационная безопасность и защита информации : 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. 3. Гришина, Н. В. Информационная безопасность предприятия : 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. 4. 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. ЭБС https://www.biblio-online.ru/viewer/836C32FD-678E-4B11-8BFC-F16354A8AFC7#page/1 5. 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. ЭБС https://www.biblio-online.ru/viewer/73BEF88E-FC6D-494A-821C-D213E1A984E1#page/1
2	Самостоятельное изучение указанных теоретических вопросов;	<ol style="list-style-type: none"> 1. «Положение о самостоятельной работе студентов»- Утвержденное 11.02.2011г. ФГБОУ ВО «КубГУ». 2. Баранова, Е. К. Информационная безопасность и защита информации : 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. 3. Гришина, Н. В. Информационная безопасность предприятия : 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.

		<p>4. 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. ЭБС https://www.biblio-online.ru/viewer/836C32FD-678E-4B11-8BFC-F16354A8AFC7#page/1</p> <p>5. 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. ЭБС https://www.biblio-online.ru/viewer/73BEF88E-FC6D-494A-821C-D213E1A984E1#page/1</p>
3	Подготовка рефератов	<p>1. «Положение о самостоятельной работе студентов»- Утвержденное 11.02.2011г. ФГБОУ ВО «КубГУ».</p> <p>2. Баранова, Е. К. Информационная безопасность и защита информации : 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.</p> <p>3. Гришина, Н. В. Информационная безопасность предприятия : 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.</p> <p>4. 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. ЭБС https://www.biblio-online.ru/viewer/836C32FD-678E-4B11-8BFC-F16354A8AFC7#page/1</p> <p>5. 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. ЭБС https://www.biblio-online.ru/viewer/73BEF88E-FC6D-494A-821C-D213E1A984E1#page/1</p>
4	Подготовка выступлений на круглом столе	<p>1. «Положение о самостоятельной работе студентов»- Утвержденное 11.02.2011г. ФГБОУ ВО «КубГУ».</p> <p>2. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие для студентов, обучающихся по направлению "Прикладная информатика" / Е. К. Баранова, А. В.</p>

		<p>Бабаш. - 3-е изд., перераб. и доп. - Москва : РИОР : ИНФРА-М, 2016. - 321 с.</p> <p>3. Гришина, Н. В. Информационная безопасность предприятия : 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.</p> <p>4. 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. ЭБС https://www.biblio-online.ru/viewer/836C32FD-678E-4B11-8BFC-F16354A8AFC7#page/1</p> <p>5. 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. ЭБС https://www.biblio-online.ru/viewer/73BEF88E-FC6D-494A-821C-D213E1A984E1#page/1</p>
5	подготовка к экзамену	<p>1. «Положение о самостоятельной работе студентов»- Утвержденное 11.02.2011г. ФГБОУ ВО «КубГУ».</p> <p>2. Баранова, Е. К. Информационная безопасность и защита информации : 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.</p> <p>3. Гришина, Н. В. Информационная безопасность предприятия : 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.</p> <p>4. 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. ЭБС https://www.biblio-online.ru/viewer/836C32FD-678E-4B11-8BFC-F16354A8AFC7#page/1</p> <p>5. 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. ЭБС https://www.biblio-online.ru/viewer/73BEF88E-FC6D-494A-821C-D213E1A984E1#page/1</p>

Примеры вопросов для самостоятельной работы обучающихся

1. Понятие информации. Фазы обращения информации в информационных системах.
2. Место информационной безопасности в национальной безопасности РФ.
3. Виды и источники угроз информационной безопасности РФ.
4. Структура государственной системы обеспечения информационной безопасности РФ.
5. Организация технической защиты информации в РФ.
6. Цели и задачи обеспечения информационной безопасности.
7. Архитектура СЗИ организации и основные требования к средствам защиты.
8. Функциональное построение СЗИ организации и назначение основных подразделений.
9. Элементарные модели СЗИ организации. Семирубежная модель защиты.
10. Последовательность и содержание основных этапов проектирования СЗИ организации.
11. Содержание процесса эксплуатации СЗИ организации.
12. Анализ угроз информационной безопасности.
13. Внутренние и внешние источники угроз информационной безопасности. Схема воздействия угроз на информационную систему.
14. Управление рисками на различных стадиях жизненного цикла информационной системы.
15. Трехмерная модель “куб безопасности”.

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.	-
Лекция	Проблемная лекция	2
Лекция	Лекция – визуализация	2
	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.

В качестве оценочных средств программой дисциплины предусматривается:

- текущий контроль в форме опроса;
- промежуточная аттестация (зачет, экзамен)

4.1 Фонд оценочных средств для проведения текущего контроля.

Вопросы 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.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Образец теста

1. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
 - а) меры обеспечения целостности;
 - б) административные меры;
 - с) меры обеспечения конфиденциальности.
2. Дублирование сообщений является угрозой:
 - а) доступности;
 - б) конфиденциальности;
 - с) целостности.
3. Вредоносное ПО Melissa подвергает атаке на доступность:
 - а) системы электронной коммерции;
 - б) геоинформационные системы;

- с) системы электронной почты.
- 4. Выберите вредоносную программу, которая открыла новый этап в развитии данной области.
 - a) Melissa.
 - b) Bubble Boy.
 - c) ILO VE YOU.
- 5. Самыми опасными источниками внутренних угроз являются:
 - a) некомпетентные руководители;
 - b) обиженные сотрудники;
 - c) любопытные администраторы.

Вопросы для подготовки к экзамену

1. Ведение в информационную безопасность
2. Угрозы кибербезопасности, уязвимости и атаки
3. Вирусы, черви и троянские кони
4. Рекламное ПО, программы-шпионы и спам
5. Защита от атак электронной почты и браузера
6. Подмена известных интернет сайтов и электронной почты
7. WEP и WPA атаки, подмена Mac адресов
8. Защита от атак мобильных устройств и беспроводных сетей
9. Принципы шифрования файлов и данных
10. Модель кибербезопасности ISO
11. Защита от атак сетевых приложений
12. Криптографические методы защиты информации
13. Локальные политики безопасности операционной системы
14. Группы пользователей и методы аутентификации
15. Разграничение доступа к информации на уровне групп пользователей
16. Доменная структура локальной сети
- 17. Политики безопасности доменов**

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. Баранова, Е. К. Информационная безопасность и защита информации : 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.
2. Гришина, Н. В. Информационная безопасность предприятия : 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.
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. ЭБС <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. ЭБС <https://www.biblio-online.ru/viewer/73BEF88E-FC6D-494A-821C-D213E1A984E1#page/1>
5. Нестеров, Сергей Александрович. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. - Москва : Юрайт, 2019. - 321 с. - <https://biblio-online.ru/viewer/informacionnaya-bezopasnost-434171#page/1> .
6. Внуков, Андрей Анатольевич. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. - 2-е изд., испр. и доп. - Москва : Юрайт, 2019. - 261 с. - <https://biblio-online.ru/viewer/zaschita-informacii-444046#page/1> .

5.2 Дополнительная литература

1. Азарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Азарин, А. С. Забабурин. — М. : Издательство Юрайт, 2017. — 312 с. — (Серия : Специалист). — ISBN 978-5-9916-9043-0. <https://www.biblio-online.ru/viewer/E458AFCD-826E-4A1F-9B4B-68BB83EA616F#page/1>
2. Зайцев, Александр Петрович. Технические средства и методы защиты информации : учебник для студентов вузов, обучающихся по группе специальностей "Информационная безопасность" / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. - 7-е изд. - Москва : Горячая линия-Телеком, 2014. - 442 с.
3. Исаев, Георгий Николаевич. Информационные системы в экономике [Электронный ресурс] : электронный учебник, вопросы и задания для самопроверки по каждой главе, расширенный список литературы / Г. Н. Исаев ; Образовательные адаптивные системы. - М. : Омега-Л, 2010. - 1 электрон. опт. диск (CD-ROM). - (Электронный учебник).
4. Современные информационно-коммуникационные технологии для успешного ведения бизнеса [Текст] : учебное пособие / [Ю. Д. Романова и др.]. - Москва : ИНФРА-М, 2014. - 178 с.
5. Исаев, Георгий Николаевич. Информационные системы в экономике [Текст] : учебник для студентов вузов / Г. Н. Исаев. - 4-е изд., стер. - М. : Омега-Л, 2011. -

462 с.

6. Балдин, Константин Васильевич. Информационные системы в экономике : учебное пособие для студентов вузов / К. В. Балдин, В. Б. Уткин. - 7-е изд. - Москва : Дашков и К°, 2017. - 395 с. - <http://znanium.com/bookread2.php?book=327836> .

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 Science (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 студента 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)
5	Консультант Плюс, Договор №177/948 от 18.05.2000

8.3 Перечень информационных справочных систем:

1. Банк России (ЦБ): www.cbr.ru.
2. Московская Межбанковская валютная биржа: www.micex.ru.
3. Федеральная служба государственной статистики: www.gks.ru
4. Информационный портал Всемирного банка: <http://data.worldbank.org>.

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 «Интернет» и обеспечением неограниченного доступа в электронную информационно-образовательную среду организации для каждого обучающегося, в соответствии с объемом изучаемых дисциплин	Кабинет для самостоятельной работы - № 504,509,510 Оборудование: персональные компьютеры, учебная мебель, доска учебная, выход в Интернет
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).

Приложение к рабочей программе дисциплины

Информационная безопасность

Направление подготовки: 38.03.05 Бизнес-информатика

Направленность (профиль): Электронный бизнес

Программа подготовки: академическая

Форма обучения: очная

Квалификация (степень) выпускника Бакалавр

8.4 Перечень профессиональных баз данных.

1. <http://www.koapp.narod.ru/russian.htm> – Электронная библиотека фонда «КОАП». На сайте представлена художественная, справочная, техническая литература (операционные системы, локальные сети), ГОСТы, ОСТы, ТУ, нормативно-справочная информация.
2. Электронный каталог Кубанского государственного университета и филиалов. – URL: <http://212.192.134.46/MegaPro/Web/Home/About>.
3. <http://www.rsl.ru> – Российская государственная библиотека (бывшая библиотека им.В.И.Ленина). На сайте можно найти различную информацию не только о фонде библиотеки РГБ, но и о других библиотечных ресурсах России. Доступ к электронным документам библиотеки платный. Условия получения доступа представлены на сайте.
4. <http://www.gpntb.ru> – Государственная публичная научно-техническая библиотека России. Предоставляется доступ в электронный каталог как самой библиотеки, так и каталоги других Московских библиотек, входящих в корпоративную сеть ГПНТБ. Предоставляются также другие услуги, узнать о которых можно на данном сайте.
5. <http://www.nlr.ru> – Российская национальная библиотека. Имеется доступ к электронным версиям различных документов.
6. <http://elibrary.ru> – Научная электронная библиотека. Предоставляет доступ для зарегистрировавшихся пользователей к электронным версиям зарубежных журналов по различным направлениям науки. Имеются как платные, так и бесплатные базы данных.
7. <http://megabook.ru/> – Наиболее полная подборка энциклопедических данных по темам: автомобили, оружие, домашние животные, здоровье, кино, компьютеры, кулинария, музыка, этикет + универсальная энциклопедия.
8. <http://www.lib.ru> – Сайт электронной библиотеки Максима Мошкова, самой известной и пополняемой. Тематический диапазон изданий широк. Наряду с произведениями художественной литературы можно посмотреть книги по многим отраслям знаний.
9. <http://diss.rsl.ru> – Электронная библиотека диссертаций Российской государственной библиотеки. Предоставляется доступ к массиву электронных версий диссертаций по различным направлениям науки. Доступ ограниченный и платный. Возможна электронная доставка необходимой Вам диссертации.
10. <http://www.infoliolib.info> – Университетская электронная библиотека. На сайте представлена учебная, научная, художественная, справочная литература по рабочим программам университетских учебных дисциплин. Ориентироваться в фондах библиотеки позволяет алфавитный каталог авторов, тематический каталог литературы по учебным дисциплинам, а также оригинальная поисковая система. Также с сайта можно выйти на ссылки других электронных библиотек.
11. <http://www.rsl.ru> – Российская государственная библиотека (бывшая библиотека им.В.И.Ленина). На сайте можно найти различную информацию не только о фонде

библиотеки РГБ, но и о других библиотечных ресурсах России. Доступ к электронным документам библиотеки платный. Условия получения доступа представлены на сайте.

12. <http://www.infoliolib.info> – Университетская электронная библиотека. На сайте представлена учебная, научная, художественная, справочная литература по рабочим программам университетских учебных дисциплин. Ориентироваться в фондах библиотеки позволяет алфавитный каталог авторов, тематический каталог литературы по учебным дисциплинам, а также оригинальная поисковая система. Также с сайта можно выйти на ссылки других электронных библиотек.

13. <http://www.kulichki.com/inkwell/>- Чернильница. Алфавитный и систематический каталоги русскоязычных фондов наиболее крупных электронных библиотек

14. <http://www.poiskknig.ru> – Поиск электронных книг. В базе данных более 67000 записей.

15. <http://old.russ.ru/krug/biblio/catalogue.html> – Лучшие электронные библиотеки: каталог.

Лист изменений и дополнений - 2018 г.

для рабочей программы дисциплины «Информационная безопасность»

<i>№</i>	<i>Внесенные изменения</i>	<i>Отметка о выполнении да /нет</i>
1	Обновление списка основной и дополнительной литературы	да
2	Добавление перечня профессиональных баз данных (п.8.4 рабочей программы)	да
3	Обновление программного обеспечения сопровождения дисциплины	да
4	Обновление материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	да
5	Обновление содержания практических (лабораторных) работ	да
6	Обновление фонда оценочных средств	да
7	Обновление форм проверки самостоятельной работы обучающихся	да
8	Обновление перечня вопросов для проведения промежуточной аттестации	да
9	Обновление перечня тем к курсовым работам	курсовая работа не предусмотрена
10	Адаптация компонентов рабочей программы для инвалидов и лиц ОВЗ	Нет (в контингенте отсутствуют инвалиды и лица с ОВЗ)

Все изменения рабочей программы рассмотрены и одобрены на заседании кафедры информатики и математики «30» августа 2018 г. Протокол № 1

Заведующий кафедрой канд. физ.-мат. наук, доцент _____



Рзун И.Г.

Лист изменений и дополнений - 2019 г.

для рабочей программы дисциплины «Информационная безопасность»

<i>№</i>	<i>Внесенные изменения</i>	<i>Отметка о выполнении да /нет</i>
1	Обновление списка основной и дополнительной литературы	да
2	Добавление перечня профессиональных баз данных (п.8.4 рабочей программы)	нет
3	Обновление программного обеспечения сопровождения дисциплины	да
4	Обновление материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	да
5	Обновление содержания практических (лабораторных) работ	нет
6	Обновление фонда оценочных средств	нет
7	Обновление форм проверки самостоятельной работы обучающихся	нет
8	Обновление перечня вопросов для проведения промежуточной аттестации	нет
9	Обновление перечня тем к курсовым работам	курсовая работа не предусмотрена
10	Адаптация компонентов рабочей программы для инвалидов и лиц ОВЗ	нет
11	Изменение титульного листа в связи с реорганизацией министерства (Министерство науки и высшего образования РФ)	да

Все изменения рабочей программы рассмотрены и одобрены на заседании кафедры информатики и математики «20» июня 2019 г. Протокол № 11

Заведующий кафедрой канд. физ.-мат. наук, доцент _____



Рзун И.Г.