МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет управления

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность
(наименование дисциплины)
Кафедра математических и естественнонаучных дисциплин
факультета __управления____

Образовательная программа

_____38.03.05 **– Бизнес-информатика**_____

Профиль подготовки
Электронный бизнес

Уровень высшего образования
_____бакалавриат_____

Форма обучения
_____очная_____

Статус дисциплины: базовая_____

Махачкала, 2016 год

Рабочая программа дисциплины «Информационная безопасность» составлена в 2016 году в соответствии с требованиями ФГОС ВО по направлению подготовки **38.03.05 – Бизнес-информатика** уровень бакалавриата

от 14.01.2010 г. №27

Разработчик: кафедра математических и естественнонаучных дисциплин, доц. Арипова Патимат Гаджиевна,

Рабочая программа дисциплины одобрена:
на заседании кафедры МиЕНД от «18» мая 2016г., протокол № 8

Зав. кафедрой Омарова П.О.

на заседании Методической комиссии факультета управления от «17» июня 2016 г., протокол № 10.

Председатель Камалова Г.А.

Рабочая программа дисциплины согласована с учебно-методическим управлением « » 2016 г.

Аннотация рабочей программы дисциплины

Учебная дисциплина «Информационная безопасность» относится к вариативной части обязательных дисциплин профессионального цикла. федерального государственного образовательного стандарта высшего профессионального образования (ФГОС ВПО) по направлению 38.03.05 Бизнес-информатика (квалификация – «бакалавр»).

Дисциплина нацелена на формирование следующей компетенции выпускника: ПК-12, ПК-22, ПК-25

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, практические занятия, самостоятельная работа.

Рабочая программа дисциплины предусматривает проведение следующих видов контроля: текущий контроль успеваемости в форме опросов, тестов, проведении письменной контрольной работы и промежуточный контроль в форме экзамена.

Объем дисциплины ___3____зачетных единиц, в том числе в 108 академических часах по видам учебных занятий

Семестр	Учебные занятия							Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен
	в том числе							
	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
	Всего	из них						
		Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
2	108	18		16			38+36	экзамен

1. Цели освоения дисциплины

Целями освоения дисциплины «Информационная безопасность» являются:

- получение базовых знаний по информационной безопасности, необходимых для решения задач, возникающих в практической деятельности специалиста;
- заложить методически правильные основы знаний по информационной безопасности, необходимых специалистам, занимающимся вопросами проектирования, внедрения и эксплуатации корпоративных информационных систем.
- дать будущим специалистам необходимые для их работы теоретические знания о современных средствах, методах и технологиях обеспечения информационной безопасности ИС;
- сформировать у студентов практические навыки организации работ по обеспечению информационной безопасности на предприятиях.
- применение системного подхода к автоматизации и информатизации решения прикладных задач, к построению информационных систем на основе современных информационно-коммуникационных технологий.

2.Место дисциплины в структуре ООП бакалавриата

Дисциплина «Информационная безопасность» относится к вариативной части обязательных дисциплин профессионального цикла. Она изучает основные методы и технологии обеспечения информационной безопасности на всех уровнях жизненного цикла информационных систем, используемых на предприятиях различных форм собственности и в органах государственного и муниципального управления.

Содержание дисциплины «Информационная безопасность» соответствует требованиям ФГОС ВПО по направлению «Бизнес-информатика)».

Дисциплина является важной составной частью теоретической подготовки специалиста по прикладной информатике и занимает существенное место в его будущей практической деятельности. Она обеспечивает возможность эффективной работы специалиста в ИТ- службах предприятий и государственных учреждений.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения) .

Компетенции	Формулировка компетенции из ФГОС ВО	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)
ПК-12	защищать права на	**знать**

	интеллектуальную собственность	• законодательную и нормативную базу ИБ; • основные меры, направленные на обеспечение ИБ на различных уровнях ИБ; **уметь** • использовать современные инструментальные средства анализа рисков • **владеть** • основными понятиями дисциплины; • навыками работы со специальной литературой;
ПК-22	консультировать заказчиков по совершенствованию бизнес-процессов и ИТ-инфраструктуры предприятия	**иметь представление** • о значении информационной безопасности для современного бизнеса; • о перспективах развития технологий обеспечения информационной безопасности; **знать** • основные меры, направленные на обеспечение ИБ на различных уровнях совершенствования бизнес-процессов; **уметь** • разрабатывать политику

		информационной безопасности предприятия; • организовывать и проводить аудит информационной безопасности; **владеть** • умением выбирать методы моделирования систем, структурировать и анализировать цели и функции систем управления;
ПК-25	консультировать заказчиков по рациональному выбору методов и инструментов управления ИТ-инфраструктурой предприятия	**иметь представление** • о методах и инструментах управления ИТ-инфраструктурой предприятия **знать** • основные методы и инструменты управления ИТ-инфраструктурой предприятия **уметь** • использовать современные методы и инструменты управления ИТ-инфраструктурой предприятия **владеть** • умением рационально выбирать методы моделирования систем, структурировать и

		анализировать цели и функции систем управления;

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет __3 зачетных единицы, _108 академических часов.

4.2. Структура дисциплины.

Название разделов и тем	Всего часов по учебному плану	Виды учебных занятий			
		Аудиторные занятия, в том числе			Самостоятельная работа
		лекции	практ	лабор	
II семестр					
Модуль I. Теоретические основы информационной безопасности.					
Раздел 1. Теоретические основы информационной безопасности.					
Тема 1. Предмет и задачи ИБ.	8	2	2		4
Тема 2. Информационная безопасность и управление рисками.	8	2	2		4
Тема 3. Административный уровень обеспечения ИБ.	10	2	2		6
Тема 4. Стандарты по ИБ.	10	2	2		6
Итого за I модуль	36	8	8		20
Модуль II Практические основы информационной безопасности.					
Раздел 2. Практические основы информационной безопасности.					
Тема 5. Механизмы обеспечения ИБ	8	2	2		4
Тема 6. Экономические аспекты обеспечения ИБ.	8	2	2		4
Тема 7. Архитектура информационной безопасности	10	2	2		6
Тема 8. Угрозы и уязвимости	10	4	2		4
Итого за II модуль	**36**	**10**	**8**		**18**
экзамен	**36**				
ИТОГО	**108**	**18**	**16**		**38**

4.3. Содержание дисциплины, структурированное по темам (разделам).

Содержание разделов дисциплины

Содержание курса.

Модуль I. Теоретические основы информационной безопасности.

Раздел 1. Теоретические основы информационной безопасности.

ТЕМА 1. Предмет и задачи информационной безопасности.

Понятие информационной безопасности. Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность. Примеры взломов информационных систем. Метрики ценности информации. Информационная безопасность (ИБ) предприятия, домашнего компьютера. Компьютерная система (КС). Исторические аспекты возникновения и развития информационной безопасности. Современные тенденции развития технологий обеспечения информационной безопасности.

ТЕМА 2. Информационная безопасность и управление рисками

Определения: уязвимости, угрозы, риски, раскрытие информации. Защита информации, субъект информационных отношений, жизненный цикл информационных систем.. Цели информационной безопасности. Технические стандарты. Типы контроля. Управление рисками и анализ рисков. Компоненты программы обеспечения информационной безопасности. Обучение персонала в области ИБ.

ТЕМА 3. Административный уровень обеспечения информационной безопасности

Политика безопасности, программа безопасности, анализ рисков, уровень детализации, карта ИС, классификация ресурсов, физическая защита, правила разграничения доступа, порядок разработки политики безопасности, оценка рисков, контроль, жизненный цикл. Практическое применение международного стандарта безопасности информационных систем ISO 17799. Типовые документы, основанные на стандарте безопасности. Управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности, планирование восстановительных работ, непрерывность защиты в пространстве и времени, физическое управление доступом, защита поддерживающей инфраструктуры, защита от перехвата данных, защита мобильных систем, поддержка пользователей, поддержка программного обеспечения, резервное копирование, управление носителями, документирование, прослеживание нарушителя, предупреждение повторных нарушений, отслеживание новых уязвимых мест, критически важные функции, идентификация ресурсов, стратегия восстановительных работ, персонал, информационная инфраструктура, физическая инфраструктура.

ТЕМА 4. Стандарты по информационной безопасности

Российские стандарты ИБ. Международные стандарты ИБ. Различия между стандартами по ИБ России, Европы и США. Доктрина информационной безопасности Российской Федерации. Законодательный уровень обеспечения информационной безопасности.

Модуль II. Практические основы информационной безопасности.

Раздел 2. Практические основы информационной безопасности.

ТЕМА 5. Экономические аспекты обеспечения информационной безопасности

Методика оценки совокупной стоимости владения для подсистемы ИБ. Границы применения методики. Технология оценки затрат на ИБ. Идентификация затрат на безопасность. Внедрение системы учета затрат на ИБ.

ТЕМА 6. Архитектура информационной безопасности

Электронный документ (ЭД). Информационная система (ИС). Несанкционированный доступ (НСД). Отказ в обслуживани]. Доступность. Целостность. Конфиденциальность. Цель и эффективность защиты информации.

Задачи ИБ предприятия. Архитектура информационной безопасности предприятия. Инфраструктура ИБ.

ТЕМА 7. Оценка защищенности компьютерных систем

Критерии оценки надежности компьютерных систем TCSEC. Критерии оценки безопасности информационных технологий ITSEC . Общие критерии оценки безопасности информационных технологий ИСО/МЭК 15408-2002. Функциональные требования к ИБ. Методы идентификации, аутентиации, авторизации и подотчетности.

ТЕМА 8. Угрозы и уязвимости

Угрозы и уязвимости безопасности информации в ИС. Атака на ИС. Непреднамеренные (случайные) и преднамеренные (умышленные) угрозы. Угрозы, связанные и не связанные с физическим доступом к элементам ИС.

Типы атак. Спам. Подбор пароля. Отказ в обслуживании. Классификация Интернет-атак по типам угроз.

5. Образовательные технологии

С целью формирования и развития профессиональных навыков обучающихся в соответствии с требованиями ФГОС ВО по направлению подготовки предусматривается широкое использование в учебном процессе активных и интерактивных форм проведения занятий:

- во время лекционных занятий используется презентация с применением слайдов с графическим и табличным материалом, что повышает наглядность и информативность используемого теоретического материала;
- практические занятия предусматривают использование групповой формы обучения, которая позволяет студентам эффективно взаимодействовать в микрогруппах при обсуждении теоретического материала;
- использование кейс–метода (проблемно–ориентированного подхода), то есть анализ и обсуждение в микрогруппах конкретной задачи;
- использование тестов для контроля знаний во время текущих аттестаций и промежуточной аттестации.

6. Учебно-методическое обеспечение самостоятельной работы студентов.

Возрастает значимость самостоятельной работы студентов. Изучение курса «Информационная безопасность» предусматривает работу с основной, специальной и с дополнительной литературой, а также выполнение презентаций и написание рефератов.

Самостоятельная работа студентов должна способствовать более глубокому усвоению изучаемого курса, формировать навыки исследовательской работы, принятия решения и ориентировать студентов на умение применять теоретические знания на практике.

Задания для самостоятельной работы, их содержание и форма контроля приведены в форме таблицы.

№ п/п	№ раздела дисциплины	Тематика самостоятельной работы *(детализация)*	Трудо-емкость (час.)	Контроль выполнения работы (Опрос, тест, дом.задание, и т.д)
1.	1	Самостоятельное изучение тем: Примеры взломов информационных систем. Компьютерная система (КС). Цели информационной безопасности. Технические стандарты. Международные стандарты ИБ. Обучение персонала в области ИБ Изучение теоретического материала, подготовка к практическим занятиям. Подготовка реферата, подготовка к контрольной работе.	**20** 2 2 2 2 2 10	Опрос на практических занятиях. Проверка рефератов. Тестирование
2.	2	Самостоятельное изучение тем: Цель и эффективность защиты информации. Функциональные требования к ИБ. Классификация Интернет-атак по типам угроз. Методы ограничения физическог\о доступа к компонентам ЭВМ Основные методы защиты от копирования. Изучение теоретического материала, подготовка к практическим занятиям. подготовка реферата, подготовка к итоговой контрольной работе.	**18** 2 2 2 2 2 4 4	Опрос на практических занятиях. Проверка рефератов. Тестирование Проверка презентации
.	Итого		38	

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

Перечень компетенций с указанием этапов их формирования приведен в описании образовательной программы.

Компетенция	Знания, умения, навыки	Процедура освоения
ПК- 12	**знать** • законодательную и нормативную базу ИБ; • основные меры, направленные на обеспечение ИБ на различных уровнях ИБ; **уметь** • использовать современные инструментальные средства анализа рисков • **владеть** • основными понятиями дисциплины; • навыками работы со специальной литературой;	Устный опрос, тестирование, написание рефератов.
ПК-22	**иметь представление** • о значении информационной безопасности для современного бизнеса; • о перспективах развития технологий обеспечения информационной безопасности; **знать** • основные меры, направленные на обеспечение ИБ на различных уровнях совершенствования бизнес-процессов; **уметь** • разрабатывать политику информационной безопасности предприятия; • организовывать и проводить аудит информационной безопасности; **владеть** • умением выбирать методы моделирования систем, структурировать и анализировать цели и функции систем управления;	Устный опрос, конспектирование законов, написание рефератов, тестирование
ПК-25	**иметь представление** • о методах и инструментах управления ИТ-инфраструктурой предприятия **знать** • основные методы и инструменты управления ИТ-инфраструктурой предприятия **уметь** • использовать современные методы и инструменты управления ИТ-инфраструктурой предприятия **владеть** • умением рационально выбирать методы моделирования систем, структурировать и анализировать цели и функции систем управления;	Устный опрос, тестирование, написание рефератов, выполнение презентаций.

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания.

ПК- 12 (защищать права на интеллектуальную собственность)

Уровень	Показатели (что	Оценочная шкала

	обучающийся должен продемонстрировать)	Удовлет-но	Хорошо	Отлично
Пороговый	**знать** • законодательную и нормативную базу ИБ; • основные меры, направленные на обеспечение ИБ на различных уровнях ИБ; **уметь** • использовать современные инструментальные средства анализа рисков **владеть** • основными понятиями дисциплины; • навыками работы со специальной литературой;	Имеет неполное представление о законодательной и нормативной базе ИБ, о основных мерах, направленных на обеспечение ИБ на различных уровнях ИБ Демонстрирует слабое владение основными понятиями дисциплины; навыками работы со специальной литературой.	Допускает неточности в понимании законодательной и нормативной базе ИБ, основных мерах, направленных на обеспечение ИБ на различных уровнях ИБ методов теории множеств, Имеет представление об основных современных инструментальных средствах анализа рисков	Демонстрирует четкое представление о законодательной и нормативной базе ИБ, о основных мерах, направленных на обеспечение ИБ на различных уровнях ИБ Четко владеет основными современными инструментальными средства анализа рисков

ПК-22 (консультировать заказчиков по совершенствованию бизнес-процессов и ИТ-инфраструктуры предприятия)

Уровень	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетворительно	Хорошо	Отлично
Пороговый	**иметь представление** • о значении информационной безопасности для современного бизнеса; • о перспективах развития технологий обеспечения информационной безопасности; **знать** • основные меры, направленные на обеспечение ИБ на различных уровнях	Имеет неполное представление о о значении информационной безопасности для современного бизнеса; Демонстрирует слабое умение разрабатывать политику информационной безопасности предприятия	Допускает неточности в знании методов и моделей теории систем и системного анализа Может проводить системный анализ прикладной области и содержательно интерпретировать получаемые количественные результаты. Владеет	Демонстрирует четкое представление о о методах и моделях теории систем и системного анализа. Может грамотно проводить системный анализ прикладной области и содержательно интерпретировать получаемые количественные результаты.

	совершенствования бизнес-процессов; **уметь** • разрабатывать политику информационной безопасности предприятия; • организовывать и проводить аудит информационной безопасности; **владеть** • умением выбирать методы моделирования систем, структурировать и анализировать цели и функции систем управления;	Слабо владеет навыками методы моделирования систем, структурировать и анализировать цели и функции систем	навыками методы моделирования систем, структурировать и анализировать цели и функции систем	Эффективно владеет навыками методы моделирования систем, структурировать и анализировать цели и функции систем

ПК-25 (консультировать заказчиков по рациональному выбору методов и инструментов управления ИТ-инфраструктурой предприятия)

Уровень	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетворительно	Хорошо	Отлично
Пороговый	**иметь представление** • о методах и инструментах управления ИТ-инфраструктурой предприятия **знать** • основные методы и инструменты управления ИТ-инфраструктурой предприятия **уметь** • использовать современные методы и инструменты управления ИТ-инфраструктурой предприятия **владеть** • умением рационально выбирать методы моделирования	Имеет неполное представление о методах и инструментах управления ИТ-инфраструктурой предприятия Демонстрирует слабое умение использовать современные методы и инструменты управления ИТ-инфраструктурой предприятия Слабо владеет умением рационально выбирать методы моделирования систем, структурировать и анализировать	Допускает неточности в методах и инструментах управления ИТ-инфраструктурой предприятия Может проводить современные методы и инструменты управления ИТ-инфраструктурой предприятия Владеет навыками рационального выбора методы моделирования систем, структурировани я и	Демонстрирует четкое представление о методах и инструментах управления ИТ-инфраструктурой предприятия Может грамотно проводить системный анализ прикладной области и содержательно интерпретировать получаемые количественные результаты. Эффективно владеет навыками рационального выбора методы моделирования

	систем, структурировать и анализировать цели и функции систем управления;	цели и функции систем управления;	анализирования целей и функции систем управления;	систем, структурирования и анализирования целей и функции систем управления;

7.3. Типовые контрольные задания

Текущий контроль успеваемости в форме опросов, тестов, письменной контрольной работы и промежуточный контроль в виде экзамена.

Тематика рефератов

1. Основные методы защиты данных от НСД.
2. Уязвимость информационных систем. Анализ рисков наиболее значительных угроз .
3. Криптосистема операционной системы Windows. Шифрование и дешифрование в CryptoAPI.
4. Анализ и составление политики безопасности.
5. 18. Практическое применение цифровой подписи.
6. 13. Вычислительная сеть как составная часть ИС. Сетевые уязвимости, угрозы и атаки.
7. Государственная система защиты информации РФ
8. Анализ мирового рынка антивирусного программного обеспечения
9. Методы и средства борьбы со спамом.
10. Компьютерная преступность в России.
11. Законодательные и правовые основы защиты компьютерной информации.
12. Анализ рынка программного обеспечения используемого для обработки конфиденциальной информации.
13. Классификация вирусов. Технологии антивирусной защиты.
14. Политика информационной безопасности в РФ
15. Анализ рынка образовательных услуг в сфере информационной безопасности
16. Анализ российского рынка программно-аппаратных средств аутентификации
17. Угрозы несанкционированного доступа к информации при помощи программных средств
18. Анализ мирового рынка систем архивирования данных
19. Аппаратные средства защиты информации
20. Алгоритмы цифровой подписи
21. Способы защиты операционных систем
22. Экономические основы защиты конфиденциальной информации

23. Классификация угроз в сфере информационной безопасности
24. Современные технологии аутентификации и управления безопасностью компания.
25. Методы и средства обеспечения безопасности ПО.

Вопросы к экзамену.

вопросы к модулю I

1. Понятие информационной безопасности.
2. Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность.
3. Компьютерная система (КС).
4. Исторические аспекты возникновения и развития информационной безопасности.
5. Защита информации, субъект информационных отношений, жизненный цикл информационных систем.
6. Цели информационной безопасности.
7. Технические стандарты. Типы контроля.
8. Управление рисками и анализ рисков.
9. Политика безопасности, программа безопасности.
10. Анализ рисков, оценка рисков, контроль, жизненный цикл.
11. Типовые документы, основанные на стандарте безопасности.
12. Непрерывность защиты в пространстве и времени.
13. Физическое управление доступом.
14. Защита поддерживающей инфраструктуры.
15. Защита от перехвата данных.
16. Российские стандарты ИБ.
17. Международные стандарты ИБ.
18. Различия между стандартами по ИБ России, Европы и США.
19. Доктрина информационной безопасности Российской Федерации.
20. Законодательный уровень обеспечения информационной безопасности.
21. Методика оценки совокупной стоимости владения для подсистемы ИБ.
22. Технология оценки затрат на ИБ.
23. Идентификация затрат на безопасность.
24. Внедрение системы учета затрат на ИБ.

вопросы к модулю II.

25. Электронный документ (ЭД).
26. Информационная система (ИС).
27. Несанкционированный доступ (НСД). Цель и эффективность защиты информации.

28. Задачи ИБ предприятия.
29. Архитектура информационной безопасности предприятия.
30. Инфраструктура ИБ.
31. Функциональные требования к ИБ.
32. Методы идентификации, аутентиации, авторизации и подотчетности.
33. Угрозы и уязвимости безопасности информации в ИС.
34. Типы атак. Отказ в обслуживании.
35. Классификация Интернет-атак по типам угроз.
36. Системы обнаружения вторжений. Системы защиты от вторжений.
37. Антиспам и антивирусные программы.
38. Методы ограничения физического доступа к компонентам ЭВМ.
39. Основные функции и методы средств защиты от копирования.
40. Сервисы безопасности.

Примерный тест

№1 Выделяют следующие уровни формирования режима информационной безопасности:

1. обеспечение доступности информации
2. нарушение целостности информации
3. законодательно-правовой, административный (организационный), программно-технический
4. обеспечение конфиденциальности информации

№2 Организационный уровень должен охватывать:

1. методы, формы и способы защиты, их правовой статус
2. задачи по обеспечению информационной безопасности для разных категорий субъектов
3. анализ потока сообщений, контроль правильности передачи сообщений, подтверждение отдельных сообщений
4. все структурные элементы систем обработки данных на всех этапах их жизненного цикла

№3 Выберите правильные утверждения:

1. разработка политики информационной безопасности ведется для конкретных условий функционирования информационной системы
2. информационная безопасность - многогранная область деятельности, в которой успех может принести только защищенность информации и поддерживающей ее инфраструктуры
3. информационная безопасность характеризует состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства
4. результатом разработки политики безопасности является комплексный

документ, представляющий систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности

№4 К аппаратным средствам относятся:

1. технические носители информации
2. публикации, документы
3. схемы контроля информации по четности
4. схемы доступа по ключу

№5 Задачей административного уровня является:

1. разработка и реализация практических мероприятий по созданию системы информационной безопасности, учитывающей особенности защищаемых информационных систем
2. разработка программы работ в области информационной безопасности и обеспечение ее выполнения в конкретных условиях функционирования информационной системы
3. правовая, организационная защита информации
4. сохранение государственной тайны, конфиденциальности документированной информации в соответствие с законодательством

№6 Политика безопасности -

1. включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений
2. это предотвращение, пресечение, противодействие несанкционированному доступу
3. это набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации
4. это всевозможные меры, пути, способы и действия, обеспечивающие упреждение противоправных действий

№7 К аппаратным средствам, подлежащим защите относятся:

1. обслуживающий персонал и пользователи
2. конфиденциальная и динамическая информация
3. компьютеры и их составные части, кабели, линии связи
4. исходные, объектные, загрузочные модули

№8 Для сервисных информационных служб реального времени важным является:

1. соблюдение конфиденциальности
2. обеспечение целостности данных
3. выявление уязвимости системы безопасности
4. обеспечение доступности подсистем

№9 Поставщики аппаратного и программного обеспечения

1. занимаются обеспечением функционирования информационной сети организации

2. несут ответственность за поддержание должного уровня информационной безопасности в поставляемых продуктах

3. являются промежуточным звеном между операторами и специалистами по информационной безопасности

4. играют основную роль в разработке и соблюдении политики безопасности предприятия

№10 Выберите правильные утверждения:

1. необходимость следования некоторым стандартам (например, криптографическим и/или Руководящим документам Гостехкомиссии России) закреплена законодательно

2. угрозы информации выражаются в предотвращении, пресечении, противодействии несанкционированному доступу.

3. СЗИ должна предоставлять пользователю минимальные полномочия, необходимые ему для выполнения порученной работы

4. технические спецификации, применимые к современным распределенным ИС, создаются главным образом, "Тематической группой по технологии Internet" и ее подразделением - рабочей группой по безопасности.

№11 Оценочные стандарты -

1. регламентирующие различные аспекты реализации и использования средств и методов защиты

2. предназначенные для оценки и классификации ИС и средств защиты по требованиям безопасности

3. определяют, как именно строить ИС предписанной архитектуры и выполнять организационные требования

4. описывают важнейшие, с точки зрения ИБ, понятия и аспекты ИС, играя роль организационных и архитектурных спецификаций

№12 Первым оценочным стандартом, получившим международное признание стал:

1. стандарт Минобороны США "Критерии оценки доверенных компьютерных систем"

2. стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"

3. стандарт "Оранжевая книга"

4. стандарт "Общие критерии"

№13 Для структуризации пространства требований в «Общих критериях» введена иерархия:

1. класс — семейство — компонент — элемент

2. семейство —класс —компонент — элемент
3. класс — семейство — элемент — компонент
4. элемент — компонент —семейство —класс

№14 Элемент -

1. это минимальный набор требований, фигурирующий как целое
2. это неделимое требование
3. в пределах класса различаются по строгости и другим тонкостям требований
4. определяют наиболее общую, «предметную» группировку требований

№15 Базовый профиль защиты

1. это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности
2. содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности
3. представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях)
4. должен включать требования к основным (обязательным в любом случае) возможностям

№16 В стандарте "Общие критерии" число классов требований доверия безопасности равно:

_____

№17 Аутентификация бывает

1. целенаправленной, конкретной
2. универсальной, комплексной
3. односторонней и двусторонней
4. независимой, целостной

№18 Целостность данных

1. подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры
2. обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети
3. обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных
4. используется при установлении соединения и периодически во время сеанса

№19 Администрирование сервисов безопасности включает в себя:

1. администрирование управления доступом (распределение информации,

необходимой для управления — паролей, списков доступа и т. п.)

2. управление маршрутизацией (выделение доверенных путей)
3. комбинирование механизмов для реализации сервисов
4. взаимодействие с другими администраторами для обеспечения согласованной работы

№20 Администрирование информационной системы в целом включает

1. обеспечение актуальности политики безопасности
2. комбинирование механизмов для реализации сервисов
3. взаимодействие с другими административными службами
4. определение защищаемых объектов

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

Оценка за модуль определяется как сумма баллов за текущую и контрольную работу.

Коэффициент весомости баллов, набранных за текущую и контрольную работу, составляет 0,5/0,5.

Текущая работа включает оценку аудиторной и самостоятельной работы.

Оценка знаний студента на практическом занятии (аудиторная работа) производится по 100-балльной шкале.

Оценка самостоятельной работы студента (выполнение домашней контрольной работы и др.) также осуществляется по 100-балльной шкале.

Для определения среднего балла за текущую работу суммируются баллы, полученные за аудиторную и самостоятельную работу, полученная сумма делится на количество полученных оценок.

Итоговый балл за текущий работу определяется как произведение среднего балла за текущую работу и коэффициента весомости.

Если студент пропустил занятие без уважительной причины, то это занятие оценивается в 0 баллов и учитывается при подсчете среднего балла за текущую работу.

Если студент пропустил занятие по уважительной причине, подтвержденной документально, то преподаватель может принять у него отработку и поставить определенное количество баллов за занятие. Если преподаватель по тем или иным причинам не принимает отработку, то это занятие при делении суммарного балла не учитывается.

Контрольная работа за модуль также оценивается по 100-балльной шкале. Итоговый балл за контрольную работу определяется как произведение баллов за контрольную работу и коэффициента весомости.

Критерии оценок аудиторной работы студентов по 100-балльной шкале:
«0 баллов» - студент не смог ответить ни на один из поставленных вопросов
«10-50 баллов» - обнаружено незнание большей части изучаемого материала, есть слабые знания по некоторым аспектам рассматриваемых вопросов

«51-65 баллов» - неполно раскрыто содержание материала, студент дает ответы на некоторые рассматриваемые вопросы, показывает общее понимание, но допускает ошибки

«66-85 баллов» - студент дает почти полные ответы на поставленные вопросы с небольшими проблемами в изложении. Делает самостоятельные выводы, имеет собственные суждения.

«86-90 баллов» - студент полно раскрыл содержание материала, на все поставленные вопросы готов дать абсолютно полные ответы, дополненные собственными суждениями, выводами. Студент подготовил и отвечает дополнительный материал по рассматриваемым вопросам.

Таблица перевода рейтингового балла в «5»-балльную шкалу

Итоговая сумма баллов по дисциплине по 100-балльной шкале	Оценка по 5-балльной шкале
0-50	Неудовлетворительно
51-65	Удовлетворительно
66-85	Хорошо
86-100	Отлично

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

Основная литература.

1. **Садердинов А. А.** Информационная безопасность предприятия : учеб. пособие Междунар. акад. наук информации, информ. процессов и технологий. - 3-е изд. - М. : Дашков и К, 2006. - 335 с.
2. **Галатенко В. А.** Стандарты информационной безопасности : курс лекций: учеб. пособие / 2-е изд. - М. : ИНТУИТ.ру, 2006. - 263 с.
3. **Белов Е. Б.** Основы информационной безопасности : [учеб. пособие для вузов] / - М. : Горячая линия - Телеком, 2006. - 544 с.
4. **Галатенко В. А.** Основы информационной безопасности : учеб. пособие для студентов вузов, обуч. по специальности 351400 "Прикл. информ." - 4-е изд. - М. ИНТУИТ.ру, 2008. - 205 с
5. **Мельников В. П.** Информационная безопасность и защита информации : учеб. пособие для студентов вузов. 5-е изд., М. : Академия, 2011. - 330с.
6. **Башлы П.Н.** Информационная безопасность / - Ростов на Дону: Феникс, 2006. - 253стр.
7. **Курило А.П.** «Обеспечение информационной безопасности бизнеса» М. БДЦ-Пресс, 2005.

Дополнительная литература

1. **Филин С. А.** Информационная безопасность : учеб. пособие / - М. : Альфа-Пресс, 2006. - 411 с.

2. **Богомолов В. А.** Экономическая безопасность : учеб. пособие для вузов / М. : ЮНИТИ-ДАНА, 2006. - 303 с.

3. **Расторгуев С. П.** Основы информационной безопасности : учеб. пособие для студентов вузов, - М. : Академия, 2007. - 186 с.

4. **Шаньгин В. Ф.** Информационная безопасность компьютерных систем и сетей : учеб. пособие для студентов - М. : ФОРУМ: ИНФРА-М, 2008. - 415 с.

5. Торстейнсон Питер. Криптография и безопасность в технологии .пер. с англ. В.Д.Хорева; - М. : БИНОМ. Лаб. знаний, 2007. - 479 с.

6. **Девянин П.Н.** «Анализ безопасности управления доступом и информационными потоками в компьютерных системах» М. Радио и связь, 2006

7. **Курило А.П., Зефиров С.Л., Голованов В.Б.** «Аудит информационной безопасности» М. БДЦ-Пресс, 2006

8. **Щербаков А. Ю.,** Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.:Книжный мир, 2009. — 352 с — ISBN 978-5-8041-0378-2.

9. **А. А. Губенков, В. Б. Байбурин.** Информационная безопасность. - Новый издательский дом, 2005 г. - 128 стр. - ISBN 5-9643-0091-X.

10. **Родичев Ю.** Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. — 272 с — ISBN 978-5-388-00069-9.

11. **Шаньгин В. Ф.** Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. — 544 с — ISBN 5-94074-383-

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

Системы программирования Mathcad, Matlab, Maple. Система дистанционного образования MOODLE для сопровождения самостоятельной работы студентов (методические материалы: текстовые, аудио и видеофайлы, индивидуальные задания, тесты и т.д.).

Профильные периодические издания

- Безопасность информационных технологий (Выпускается МИФИ. Является рецензируемым научным журналом, включенным в список ВАК)
- Вопросы защиты информации
- Проблемы информационной безопасности. Компьютерные системы (Является рецензируемым научным журналом, включенным в список ВАК)
- Jet Info информационный бюллетень
- Журнал «Защита информации. Инсайд»
- InformationSecurity: Информационная безопасность
- Журнал, посвященный компьютерной безопасности
- Информационная безопасность
- Информационная безопасность — OSP News

Специализированные порталы

- SecurityLab.ru
- Независимый информационно-аналитический портал по безопасности
- SASecurity Information Box
- Информационная безопасность на Report.ru
- Информационная безопасность / Блог / Хабрахабр
- Библиотека информационной безопасности
- Библиотека сетевой безопасности
- Компьютерная безопасность: уязвимости, ошибки и эксплоиты
- Построение безопасности в сетях
- openPGP в России
- Защита информации
- Управление доступом пользователей к сетевым ресурсам и рабочим станциям

в) Программное обеспечение и интеренет-ресурсы:

Система дистанционного образования MOODLE для сопровождения самостоятельной работы студентов (методические материалы: текстовые, аудио и видеофайлы, индивидуальные задания, тесты и т.д.).

Информационные образовательные ресурсы включают электронные учебно-методические комплексы (УМК), обеспечивающие эффективную работу обучающихся по всем видам занятий в соответствии с учебным планом.

При использовании Интернет-технологий в индивидуальном обучении обучающийся должен использовать ИКТ, соответствующие требованиям (канал связи, аппаратные требования, программные требования), предъявляемым образовательным учреждением к обучению с использованием ДОТ.

10. Методические указания для обучающихся по освоению дисциплины.

Учебный материал дисциплины «Информационная безопасность» состоит из следующих разделов: 1)Теоретические основы ИБ; 2)Практические основы ИБ.

Для успешного освоения учебного материала курса «Информационная безопасность» требуются систематическая работа по изучению лекций и рекомендуемой литературы, подготовка рефератов, а также активное участие в работе семинаров.

Изучение раздела «Теоретические основы ИБ» служит углубленному изучению основных составляющих информационной безопасности. Здесь изучаются исторические аспекты возникновения и развития информационной безопасности, стандарты по информационной безопасности. Рассматриваются современные тенденции развития технологий обеспечения информационной безопасности.

При изучении раздела "Практические основы ИБ " исследуются: программно-технический уровень обеспечения информационной безопасности, архитектура информационной безопасности, оценка защищенности компьютерных систем.

Форма проведения занятий: лекции, практические (семинарские) занятия.

Форма контроля:

- *текущий контроль* осуществляется устными опросами на занятиях, тестированием по конкретным темам, проверкой рефератов.
- *контроль* знаний студентов осуществляется с помощью 2-х письменных модульных контрольных работ.
- в конце семестра проводится экзамен.
- итоговая оценка определяется суммой баллов за экзаменационную письменную работу и средним баллом за модули.

Итоговая оценка за экзамен выставляется в форме «неудовлетворительно», «удовлетворительно», «хорошо», «отлично» и в баллах по 100-балльной шкале:

- «неудовлетворительно» - менее 51 балла;
- «удовлетворительно» - от 51 до 65 баллов;
- «хорошо» - от 66 до 85 баллов;
- «отлично» - от 86 до 100.

Методические рекомендации для преподавателя

Основным методом изучения тем, вынесенных в лекционный курс, является информационно-объяснительный метод с элементами проблемных ситуаций и заданий студентам. На практических занятиях основным является поисковый метод, связанный с решением различных типов задач.

Средствами обучения является базовые учебники, дополнительные пособия для организации самостоятельной работы студентов, демонстрационные материалы, сборники задач.

Приемами организации учебно-познавательной деятельности студентов являются приемы, направленные на осмысление и углубление предлагаемого содержания и приемы, направленные на развитие аналитико-поисковой и исследовательской деятельности.

Важно четко представлять структуру курса, уметь выделить в каждом разделе основные, базовые понятия, обозначенные минимумом содержания, определенного государственным образовательным стандартом.

Критерии оценок

В основе оценки знаний по предмету лежат следующие основные требования:

- освоение всех разделов теоретического курса Программы;
- умение применять полученные знания к решению конкретных задач.

Ответ заслуживает ***отличной оценки***, если экзаменуемый показывает знания, в полной степени, отвечающие предъявляемым к ответу требованиям: это требование основных понятий и приемов решения задач. Отличная оценка характеризует свободную ориентацию экзаменуемого в предмете. Ответы на вопросы, в том числе и дополнительные, должны обнаруживать уверенное владение терминологией, основными умениями и навыками.

Хорошая оценка характеризует тот ответ, который не в полной степени удовлетворяет вышеперечисленным критериям, однако, экзаменуемый обнаруживает прочные знания в объеме курса. Ответ должен быть достаточно аргументирован, вопросы глубоко и осмысленно изложены.

Оценка «***удовлетворительно***» выставляется за то, что ответ экзаменуемого соотносится с основными требованиями, т.е. имеются в виду твердые знания в объеме учебной программы и умение владеть терминологией. Удовлетворительная оценка выставляется за знание в целом, однако, отдельные детали могут быть упущены.

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

Для проведения индивидуальных консультаций может использоваться электронная почта. Разрабатывается учебный курс на электронной платформе Moodle.

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

На факультете управления Дагестанского государственного университета имеются аудитории (405 ауд., 421 ауд., 408 ауд., 434 ауд.), оборудованные интерактивными, мультимедийными досками, проекторами, что позволяет читать лекции в формате презентаций, разработанных с помощью пакета прикладных программ MS Power Point, использовать наглядные, иллюстрированные материалы, обширную информацию в табличной и графической формах, пакет прикладных обучающих программ, а также электронные ресурсы сети Интернет.