

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет управления
кафедра бизнес-информатики и высшей математики

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Образовательная программа
38.03.05 «Бизнес-информатика»

Профиль подготовки
«Технологическое предпринимательство»
«Электронный бизнес»

Уровень высшего образования
Бакалавриат

Форма обучения
Очная

Статус дисциплины: вариативная

Махачкала, 2019 год

Содержание

Аннотация рабочей программы дисциплины	4
1. Цели освоения дисциплины	5
2. Место дисциплины в структуре ОПОП бакалавриата.....	5
3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения)	5
4. Объем, структура и содержание дисциплины.	7
5. Образовательные технологии	12
6. Учебно-методическое обеспечение самостоятельной работы студентов.	13
7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.	15
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.....	25
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.	26
10. Методические указания для обучающихся по освоению дисциплины.	27
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.	29
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.....	29

Аннотация рабочей программы дисциплины

Учебная дисциплина «Информационная безопасность» относится к вариативной части обязательных дисциплин образовательной программы бакалавриата и является важной составной частью теоретической подготовки специалиста в области технологического предпринимательства и занимает существенное место в его будущей практической деятельности.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций по направлению 38.03.05- Бизнес-информатика «БАКАЛАВР» и профилям подготовки «Технологическое предпринимательство», «Электронный бизнес».

Дисциплина нацелена на формирование следующих компетенций выпускника: ОК-1, ПК-9, ПК- 11.

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 ___4___ зачетных единиц, в том числе в 144 академических часах по видам учебных занятий

Семес тр	Учебные занятия						СРС, в том числе экзамен	Форма промежуточной аттестации (зачет, дифференциро ванный зачет, экзамен
	в том числе							
	Контактная работа обучающихся с преподавателем							
	Всег о	из них						
		Лекц ии	Лабораторн ые занятия	Практиче ские занятия	КСР	консульта ции		
1	144	16		16			76+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 ОПОП бакалавриата

Дисциплина «Информационная безопасность» относится к вариативной части обязательных дисциплин образовательной программы бакалавриата по направлению 38.03.05- Бизнес-информатика, профиль подготовки «Технологическое предпринимательство», «Электронный бизнес» и является важной составной частью теоретической подготовки специалиста в области технологического предпринимательства. 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 и 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)
ОПК-1	способность решать стандартные задачи профессиональной деятельности на основе информационной и	знать <ul style="list-style-type: none">• основные понятия современной информационной и

	<p>библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p>	<p>библиографической культуры;</p> <ul style="list-style-type: none"> • основные методы применения ИКТ и с учетом основных требований ИБ; <p>уметь</p> <ul style="list-style-type: none"> • использовать современные навыки информационной и библиографической культуры <p>владеть</p> <ul style="list-style-type: none"> • основными понятиями дисциплины; • навыками работы со специальной литературой;
ПК-9	<p>организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия</p>	<p>иметь представление</p> <ul style="list-style-type: none"> • значения информационной безопасности для современного бизнеса; <p>знать</p> <ul style="list-style-type: none"> • основные меры, направленные на управление ИБ ИТ-инфраструктуры предприятия; <p>уметь</p> <ul style="list-style-type: none"> • разрабатывать способы взаимодействия с клиентами и партнерами в процессе решения задач; <p>организовывать и проводить аудит</p>

		<p>информационной безопасности ИТ-инфраструктуры предприятия;</p> <p>владеть</p> <ul style="list-style-type: none"> • навыками взаимодействия с клиентами и партнерами в процессе решения задач управления ИБ ИТ-инфраструктуры предприятия
ПК-11	защищать права на интеллектуальную собственность	<p>знать</p> <ul style="list-style-type: none"> • законодательную и нормативную базу ИБ; • основные меры, направленные на обеспечение ИБ на различных уровнях ИБ; <p>уметь</p> <ul style="list-style-type: none"> • использовать современные инструментальные средства анализа рисков • владеть • основными понятиями дисциплины; • навыками работы со специальной литературой;

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет __4 зачетных единицы, _144 академических часов.

4.2. Структура дисциплины.

№ п/п	Разделы и темы дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные занятия	КСР		
Модуль I. Теоретические основы информационной безопасности.									
Раздел 1. Теоретические основы информационной безопасности.									
1	Тема 1. Предмет и задачи ИБ.	1	1	2	2			8	Фронтальный опрос, тестирование
2	Тема 2. Информационная безопасность и управление рисками.	1	2	2	2			8	Опрос, тестирование, защита реферата
3	Тема 3. Административный уровень обеспечения ИБ.	1	3-4	2	2			8	Опрос, тестирование, защита реферата
Итого по модулю 1		36	1-4	6	6			24	Контрольная работа
Модуль II Практические основы информационной безопасности.									
Раздел 2. Практические основы информационной безопасности.									
4	Тема 4. Стандарты по ИБ.	1	4-5	2	4			12	Опрос, тестирование, защита реферата
5	Тема 5. Механизмы обеспечения ИБ	1	5-6	2	2			14	Фронтальный опрос, решение кейсов и задач, тестирование, защита рефератов
Итого по модулю 2		36		4	6			26	Контрольная работа
Модуль III Экономические основы информационной безопасности.									
6	Тема 6. Угрозы и уязвимости.			2	2			12	
6	Тема 7. Экономические аспекты обеспечения ИБ.	6	7	2	2			8	Опрос, решение кейсов и задач, тестирование, защита рефератов
	Тема 8. Архитектура ИБ			2				6	
Итого по модулю 3		36	5-10	6	4			26	Контрольная работа
9	Модуль 4 подготовка к экзамену							36	Экзамен

	Всего за семестр	144		16	16			76+ 36	Экзамен
--	-------------------------	------------	--	-----------	-----------	--	--	-------------------------	----------------

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

4.3.1. Содержание лекционных занятий по дисциплине.

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.

Модуль II. Практические основы информационной безопасности.

Раздел 2. Практические основы информационной безопасности.

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.

ТЕМА 5. Механизмы обеспечения ИБ

Идентификация и аутентификация. Методы аутентификации. Криптография и шифрование. Криптографические методы. Открытые и закрытые ключи. Способы генерации ключей. Методы разграничения доступа. Регистрация и аудит. Межсетевое экранирование.

Модуль III. Экономические основы информационной безопасности.

Раздел 3. Экономические основы информационной безопасности.

ТЕМА 6. 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.

Тема 7. 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 8. Архитектура информационной безопасности

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

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

4.3.2. Содержание практических занятий по дисциплине.

Модуль I. Теоретические основы информационной безопасности.

Раздел 1. Теоретические основы информационной безопасности.

ТЕМА 1. Предмет и задачи информационной безопасности. *(семинар)*

1. Основные составляющие информационной безопасности.
2. Исторические аспекты возникновения и развития информационной безопасности.
3. Современные тенденции развития технологий обеспечения информационной безопасности.

Ссылка на учебно-методическую литературу, указанную в п.8

ТЕМА 2. Информационная безопасность и управление рисками. *(семинар)*

1. Уязвимости, угрозы, риски, раскрытие информации.
2. Управление рисками и анализ рисков.
3. Компоненты программы обеспечения информационной безопасности.

Ссылка на учебно-методическую литературу, указанную в п.8

ТЕМА 3. Административный уровень обеспечения информационной безопасности.

1. Политика безопасности, программа безопасности, анализ рисков.
2. Типовые документы, основанные на стандарте безопасности.
3. Информационная инфраструктура.

Ссылка на учебно-методическую литературу, указанную в п.8

Модуль II. Практические основы информационной безопасности.

Раздел 2. Практические основы информационной безопасности.

ТЕМА 4. Стандарты по информационной безопасности. *(семинар)*

1. Стандарты по информационной безопасности
2. Международные стандарты по информационной безопасности
3. Стандарты РФ.

Ссылка на учебно-методическую литературу, указанную в п.8

ТЕМА 5. Механизмы обеспечения ИБ

1. Идентификация и аутентификация. Методы аутентификации.
2. Криптография и шифрование. Криптографические методы. Открытые и закрытые ключи. Способы генерации ключей.

3. Методы разграничения доступа.
4. Регистрация и аудит.
5. Межсетевое экранирование.

Ссылка на учебно-методическую литературу, указанную в п.8

ТЕМА. 6. Угрозы и уязвимости. (семинар)

1. Методы идентификации, авторизации и подотчетности.
2. Угрозы и уязвимости.
3. Типы атак.

Ссылка на учебно-методическую литературу, указанную в п.8

Тема 7. Экономические аспекты обеспечения информационной безопасности

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

Ссылка на учебно-методическую литературу, указанную в п.8

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 ситуации;
- 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.

Основными видами самостоятельной работы студентов в рамках освоения дисциплины выступают следующие:

- 1) проработка учебного материала;
- 2) работа с электронными источниками;
- 3) тестирование и выполнение кейс-заданий;
- 4) устный опрос
- 5) написание рефератов.

Виды и формы контроля самостоятельной работы студентов в рамках освоения дисциплины

Разделы дисциплины	Виды самостоятельной работы (и ссылки на литературу ¹)	Количество часов	Форма контроля
Раздел 1. Теоретические основы информационной безопасности	проработка учебного материала, устный опрос, работа с электронными источниками, выполнение кейс-заданий, обработка аналитических данных, работа с тестами и вопросами, написание рефератов. (1,2,3,4,7,8,9, 11,12)	26	Тестирование, устный опрос, обсуждение докладов, защита рефератов
Раздел 2. Практические основы информационной безопасности.	проработка учебного материала, устный опрос, работа с электронными источниками, выполнение кейс-заданий, работа с тестами и вопросами, написание рефератов. (1,2,3,4,7,8,9, 11,12, 16,17)	24	Тестирование, устный опрос, обсуждение презентаций, защита рефератов
Раздел 3. Экономические основы информационной безопасности.	проработка учебного материала, устный опрос, работа с электронными источниками, выполнение кейс-заданий, работа с тестами и вопросами, написание рефератов. (1,2,3,4,7,8,9, 11,12, 16,17)	26	Тестирование, устный опрос, обсуждение презентаций, защита рефератов
Итого		76	

¹ Дается ссылка на учебно-методическую литературу, указанную в п. 8.

Целью подготовки реферата является приобретение навыков творческого обобщения и анализа имеющейся литературы по рассматриваемым вопросам, что обычно является первым этапом самостоятельной работы. По каждому модулю предусмотрены написание и защита одного реферата. Тему реферата студент выбирает самостоятельно из предложенной тематики или может выбрать тему самостоятельно. Реферат должен включать введение, несколько вопросов, посвященных рассмотрению темы, заключение и список использованной

литературы. В вводной части реферата следует указать основания, послужившие причиной выбора данной темы, отметить актуальность рассматриваемых в реферате вопросов. В основном разделе излагаются наиболее существенные сведения по теме, производится их анализ, отмечаются отдельные недостатки или нерешенные еще вопросы. В заключении реферата на основании изучения литературных источников должны быть сформулированы краткие выводы и предложения. Список литературы оформляется в соответствии с требованиями ГОСТ 7.1-84 «Библиографическое описание документа». Перечень литературы составляется в алфавитном порядке фамилий первых авторов, со сквозной нумерацией. Примерный объем реферата 15-20 страниц.

Материал в реферате располагается в следующей последовательности:

- титульный лист;
- введение;
- текст работы (разбитый на разделы);
- заключение
- список литературы.

Содержание реферата студент докладывает на практическом занятии, заседании научного кружка, научно-практической конференции. На основе обсуждения студенту выставляется соответствующий балл за СРС.

Предусмотрено проведение индивидуальной работы (консультаций) со студентами в ходе изучения материала данной дисциплины.

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.

Код компетенции из ФГОС ВО	Наименование компетенции и из ФГОС ВО	Планируемые результаты обучения	Процедура освоения
ОПК-1	способность решать стандартные задачи профессиональной деятельности и на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	<p>знать</p> <ul style="list-style-type: none"> • основные понятия современной информационной и библиографической культуры; • основные методы применения ИКТ и с учетом основных требований ИБ; <p>уметь</p> <ul style="list-style-type: none"> • использовать современные навыки информационной и библиографической культуры <p>владеть</p> <ul style="list-style-type: none"> • основными понятиями дисциплины; • навыками работы со специальной литературой; 	Устный опрос, тестирование, написание рефератов.
ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры	<p>иметь представление</p> <ul style="list-style-type: none"> • значении информационной безопасности для современного бизнеса; <p>знать</p> <ul style="list-style-type: none"> • основные меры, направленные на управление ИБ ИТ-инфраструктуры предприятия; <p>уметь</p> <ul style="list-style-type: none"> • разрабатывать способы взаимодействия с клиентами и партнерами в процессе решения задач; 	Устный опрос, тестирование, написание рефератов.

	предприятия	<ul style="list-style-type: none"> • организовывать и проводить аудит информационной безопасности ИТ-инфраструктуры предприятия; <p>владеть</p> <ul style="list-style-type: none"> • навыками взаимодействия с клиентами и партнерами в процессе решения задач управления ИБ ИТ-инфраструктуры предприятия 	
ПК- 11	защищать права на интеллектуальную собственность	<p>знать</p> <ul style="list-style-type: none"> • законодательную и нормативную базу ИБ; • основные меры, направленные на обеспечение ИБ на различных уровнях ИБ; <p>уметь</p> <ul style="list-style-type: none"> • использовать современные инструментальные средства анализа рисков • владеть • основными понятиями дисциплины; • навыками работы со специальной литературой; 	Устный опрос, тестирование, написание рефератов.

7.2. Типовые контрольные задания

Текущий контроль успеваемости в форме опросов, тестов, письменной контрольной работы и промежуточный контроль в форме 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 1

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.

вопросы к модулю 2

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 3.

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, аутентификации, 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 соответствии 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 текущую работу определяется как произведение среднего балла за текущую работу и коэффициента весомости.

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.

В качестве оценочных средств программой дисциплины предусматриваются:

- посещаемость занятий;
- активное участие на практических занятиях;
- выполнение домашних и самостоятельных работ.

Весовой коэффициент - **0,5**.

текущий контроль освоения учебного материала по каждому модулю проводится в форме письменной контрольной работы с элементами тестирования и оценивается в 100 баллов.

Весовой коэффициент - **0,5**.

Максимальное количество баллов по каждому модулю - **100** баллов.

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

Форма контроля:

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

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

Критерии выставления экзаменационной оценки

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.

Неудовлетворительная оценка выставляется, если ответ не удовлетворяет хотя бы одному из требований или отсутствуют знания основных понятий и методов решения задач.

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

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

Основная литература.

1. А. А. Губенков, В. Б. Байбурун. Информационная безопасность. - Новый издательский дом, 2005 г. - 128 стр. - ISBN 5-9643-0091-X.
2. Башлы П.Н. Информационная безопасность / - Ростов на Дону: Феникс, 2006. - 253стр.
3. Курило А.П. «Обеспечение информационной безопасности бизнеса» М. БДЦ-Пресс, 2005.
4. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. — 272 с — ISBN 978-5-388-00069-9.
5. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]/ Фаронов А.Е.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 154 с.— Режим доступа: <http://www.iprbookshop.ru/52160.html>(01.09.2018)
6. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. — 544 с — ISBN 5-94074-383-
7. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 с.— Режим доступа: <http://www.iprbookshop.ru/63594.html>(01.09.2018)
8. Щербаков А. Ю., Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.:Книжный мир, 2009. — 352 с — ISBN 978-5-8041-0378-2.

Дополнительная литература

9. Бабащ, Александр Владимирович. Информационная безопасность : лаб. практикум; учеб. пособие / Бабащ, Александр Владимирович, Е. К. Баранов. - 2-е изд., стер. - И. : Кнорус, 2016, 2011. - 306-00.
10. Белов Е. Б. Основы информационной безопасности : [учеб. пособие для вузов] / - М. : Горячая линия - Телеком, 2006. - 544 с.
11. Галатенко В. А. Основы информационной безопасности : учеб. пособие для студентов вузов, обуч. по специальности 351400 "Прикл. информ." - 4-е изд. - М. ИНТУИТ.ру, 2016. - 205 с. (Основы информационных технологий). - Рекомендовано УМО. - ISBN 978-5-94774-821-5 : 230-00.

12. **Мельников** В. П. Информационная безопасность и защита информации : учеб.пособие для студентов вузов. 5-е изд., М. : Академия, 2011. - 330с. (Высшее профессиональное образование. Информатика и вычислительная техника). - Допущено УМО. - ISBN 978-5-7695-7738-3 : 401-06
13. Основы информационной безопасности : [учеб. пособие для вузов] / Е. Б. Белов. - М. : Горячая линия - Телеком, 2006. - 544 с. - ISBN 5-93517-292-5 : 154-00.
Фомин Д.В. Информационная безопасность [Электронный ресурс]: учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения/ Фомин Д.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 54 с.— Режим доступа: <http://www.iprbookshop.ru/77320.html>(01.09.2018)
7. Стандарты информационной безопасности : курс лекций: учеб. пособие / Галатенко, Владимир Антонович ; под ред. В.Б.Бетелина; Интернет-ун-т информ. технологий. - 2-е изд. - М. : ИНТУИТ.ру, 2006. - 263 с. - (Основы информационных технологий). - ISBN 5-9556-0053-1 : 176-00.
14. Информационная безопасность предприятия : учеб. пособие / Садердинов, А. А. ; В.А.Трайнёв, А.А.Федулов; Междунар. акад. наук информации, информ. процессов и технологий. - 3-е изд. - М. : Дашков и К, 2006. - 335 с. - ISBN 5-94798-918-2 : 154-00.
15. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей : учеб.пособие для студентов - М. : ФОРУМ: ИНФРА-М, 2008. - 415 с.

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)
- [JetInfo 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](#)
- [SASecurityInformationBox](#)
- [Информационная безопасность на Report.ru](#)
- [Информационная безопасность / Блог / Хабрахабр](#)
- [Библиотека информационной безопасности](#)
- [Библиотека сетевой безопасности](#)
- [Компьютерная безопасность: уязвимости, ошибки и эксплойты](#)
- [Построение безопасности в сетях](#)
- [openPGP в России](#)
- [Защита информации](#)
- [Управление доступом пользователей к сетевым ресурсам и рабочим станциям](#)

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. 3) Экономические 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.

Оптимальным путем освоения дисциплины является посещение всех лекций и семинаров и выполнение предлагаемых заданий в виде рефератов, докладов, тестов, кейс-заданий и устных вопросов.

На лекциях рекомендуется деятельность студента в форме активного слушания, т.е. предполагается возможность задавать вопросы на уточнение понимания темы и рекомендуется конспектирование основных положений лекции. На практических занятиях деятельность студента заключается в активном обсуждении вопросов темы, докладов, рефератов, решении ситуационных задач, кейсов, выполнении контрольных заданий и т.п.

При подготовке к практическому занятию студенты должны изучить конспект лекций по заданной теме, ознакомиться с соответствующим разделом в учебнике (законодательном документе), рекомендованном в качестве основной литературы. Студент может ознакомиться и с дополнительной литературой: периодические издания, интернет-источники.

Форма работы с литературой может быть разнообразной – начиная от комментированного чтения и кончая выполнением различных заданий на основе прочитанной литературы. Например; составление плана, подбор выписок из литературы по заданным вопросам; конспектирование текста.

Подготовка к экзамену предполагает изучение конспектов лекций, рекомендуемой литературы, повторение материалов практических занятий

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, Интернет-ресурсы.

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.

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

При подготовке к практическим занятиям, а также при написании рефератов могут использоваться поисковые сайты сети «Интернет», информационно-справочные системы.

Программное обеспечение: MicrosoftWindows 7, MicrosoftWord используется для создания текстовых файлов (рефератов, курсовых, выпускных квалификационных работ); MicrosoftExcel 2007 для составления аналитических таблиц и расчета показателей; PowerPoint – для создания презентаций, визуального сопровождения докладов, MicrosoftInternetExplorer – в целях поиска информации для самостоятельной работы.

Для проведения индивидуальных консультаций может использоваться электронная почта.

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

Минимально необходимый для реализации ОПОП бакалавриата перечень материально-технического обеспечения должен включать в себя:

компьютерные классы, оборудованные современными лицензионными программно-техническими средствами;

- кабинеты для интерактивного обучения;

Возможность работать в компьютерном классе из расчёта один компьютер на студента.

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 PowerPoint, использовать наглядные, иллюстрированные материалы, обширную информацию в табличной и графической формах, пакет прикладных обучающих программ, а также электронные ресурсы сети Интернет.