МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
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 бакалавриата
38.03.05 «Бизнес-информатика»

Профиль подготовки
Корпоративные информационные системы

Форма обучения
Очная

Статус дисциплины: *входит в обязательную часть*

Махачкала
2022 г.

Рабочая программа дисциплины Информационная безопасность составлена в 2022 году в соответствии с требованиями ФГОС ВО - бакалавриат по направлению подготовки: 38.03.05 Бизнес-информатика от «29» июля 2020 г. № 838.

Разработчик(и): Арипова П.Г., к.э.н., доц., кафедры БИиВМ

Рабочая программа дисциплины одобрена:
на заседании кафедры БИиВМ от «16» 03 2022г., протокол № 7

Зав. кафедрой _____ Омарова Н.О,
(подпись)

на заседании Учебно-методической комиссии факультета управления
от «16» 03 2022г., протокол № 6

Председатель _____ Гашимова Л.Г.

Рабочая программа дисциплины согласована с учебно-методическим управлением «31» 03 2022г.

Начальник УМУ _____ Гасангаджиева А.Г.
(подпись)

Содержание

Аннотация рабочей программы дисциплины

Учебная дисциплина «Информационная безопасность» входит в базовый модуль направления обязательной части Блока 1 образовательной программы по направлению подготовки 38.03.05–Бизнес-информатика (уровень бакалавриата), и является важной составной частью теоретической подготовки специалиста в области КИС и занимает существенное место в его будущей практической деятельности.

Дисциплина реализуется на факультете управления кафедрой бизнес-информатики и высшей информатики.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций по направлению 38.03.05- Бизнес-информатика «БАКАЛАВР» профилю подготовки «Корпоративные информационные системы».

Дисциплина нацелена на формирование следующихкомпетенцийвыпускника: УК-2, ОПК-1, ОПК- 2.

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, проведенииписьменной контрольной работы и промежуточный контроль в форме экзамена.

Объем дисциплины ___4____зачетных единиц, в том числе в144 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	144	16		24			68+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» входит в базовый модуль направления обязательной части Блока 1 образовательной программы по направлению подготовки 38.03.05–Бизнес-информатика (уровень бакалавриата)профиль подготовки «Корпоративные информационные системы»и является важной составной частью теоретической подготовки специалиста в его профессиональной области. 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).

Код и наименование компетенции из ФГОС ВО	**Код и наименование индикатора достижения компетенций** *(в соответствии с ПООП (при наличии))*	**Планируемые результаты обучения**	**Процедура освоения**

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.И-1. Понимает базовые принципы постановки задач и выработки решений. УК-2.И-2. Выбирает оптимальные способы решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.	**Знает** ✓ необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения **Умеет** ✓ анализировать альтернативные варианты решений для достижения намеченных результатов; ✓ разрабатывать план, определять целевые этапы и основные направления работ **Владеет** ✓ методиками разработки цели и задач проекта; ✓ методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах	Устный опрос, письменный опрос, тестирование.
ОПК-1. Способен проводить моделирование, анализ и совершенствование бизнес-процессов и информационно-технологической инфраструктуры предпри	ОПК-1. И-1. Выявляет возможности для достижения предприятием своих стратегических целей за счет использования информационных систем и информационных технологий. ОПК-1. И-2. Совершенствует процессы организации за счет использования информационных систем и информацион	**Знает** ✓ методы интегрированного представления целей предприятия, процессов, информационных систем и ИТ-инфраструктуры в рамках архитектурного подхода; ✓ основные понятия и методы работы с вычислительным оборудованием, системами хранения данных, центрами обработки данных, с сетями передачи данных. **Умеет** ✓ выявлять и реализовывать возможности для совершенствования предприятия за счет использования информационных систем и информационных технологий; ✓ совершенствовать процессы организации за счет использования информационных систем и информационных	Устный опрос, письменный опрос, тестирование.

ятия в интересах достижения его стратегических целей с использованием современных методов и программного инструментария	ных технологий. ОПК-1. И-3. Применяет инструментальные средства для моделирования текущего и целевого состояний архитектуры предприятия.	технологий; **Владеет** ✓ способами применения облачных вычислений в области инфраструктурных решений; ✓ навыками моделирования, текущего и целевого состояние архитектуры предприятия с использованием инструментальных средств.	
ОПК-2. Способен проводить исследование и анализ рынка информационных систем и информационно-коммуникационных технологий, выбирать рациональные решения	ОПК-2. И-1. Осуществляет анализ рынка информационно-коммуникационных технологий. ОПК-2. И-2. Способен выявить бизнес-потребности в информационном обеспечении и формализовать требования к ИТ-решениям. ОПК-2. И-3. Умеет анализировать и документировать различные альтернативные варианты решений для удовлетворен	**Знает** ✓ современное состояние рынка информационно-коммуникационных технологий; ✓ методы и способы проведения анализа рынка ИС и ИКТ; ✓ основные принципы организации продаж ИТ продуктов **Умеет** ✓ анализировать и документировать пригодность различных вариантов решений, выявлять и оценивать альтернативные решения; ✓ интегрировать и настраивать готовые ИТ-решения; ✓ применять на практике способы и методы анализа рынка ИС и ИКТ; ✓ выполнять анализ результатов технологических исследований в интересах серии продуктов ✓ разрабатывать предложения по приобретению и продаже ИТ продуктов. **Владеет** ✓ постановкой задачи на технологические исследования;	Устный опрос, письменный опрос, тестирование.

для управления бизнесом.	ия потребностей бизнеса. ОПК-2.И-4. Оценивает альтернативные решения в контексте их использования.	✓ координированием технологических исследований; ✓ приемами и методами технологических исследований; ✓ анализом результатов технологических исследований; ✓ исследованием существующих на рынке технологий, продуктов и организаций, как потенциальных активов для приобретения.	

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	Опрос, тестирование, защита реферата, дискуссия
2	Тема 2. Информационная безопасность и управление рисками.	1	2	2	2			8	Опрос, тестирование, защита реферата, дискуссия
3	Тема 3. Административный уровень обеспечения ИБ.	1	3-4	2	4			6	Опрос, тестирование, защита реферата, дискуссия
	Итого по модулю 1	**36**	**1-4**	**6**	**8**			**22**	Тестирование, коллоквиум
	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, дискуссия
5	Тема 5. Механизмы обеспечения ИБ	1	5-6	2	4			12	Опрос, тестирование, защита реферата, дискуссия
	Итого по модулю 2	**36**		**4**	**8**			**24**	Тестирование, коллоквиум
Модуль III Экономические основы информационной безопасности.									
Раздел 3. Экономические основы информационной безопасности.									
6	Тема 6. Угрозы и уязвимости.			2	4			10	Опрос, тестирование, защита реферата, дискуссия
6	Тема 7. Экономические аспекты обеспечения ИБ.	6	7	2	2			6	Опрос, тестирование, защита реферата, дискуссия
	Тема 8. Архитектура ИБ			2	2			6	Опрос, тестирование, защита реферата, дискуссия
	Итого по модулю 3	**36**	**5-10**	**6**	**8**			**22**	Тестирование, коллоквиум
Модуль 4. Подготовка к экзамену.									
9	Подготовка к экзамену							36	Экзамен
	Всего за семестр	**144**		**16**	**24**			**68+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

ТЕМА 8. Архитектура информационной безопасности

1. Электронный документ (ЭД). Информационная система (ИС).
2. Несанкционированный доступ (НСД). Отказ в обслуживании. Доступность. Целостность. Конфиденциальность. Цель и эффективность защиты информации.
3. Задачи ИБ предприятия. Архитектура информационной безопасности предприятия. Инфраструктура ИБ.

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 навыкиисследовательской работы, принятиярешения 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;
4) устный опрос;

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)*	22	Опрос, тестирование, дискуссия
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	Опрос, тестирование, дискуссия
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)*	22	Опрос, тестирование, дискуссия
Итого		**68**	

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

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

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

7.1. Типовые контрольные задания

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

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.

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, 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 кон-

кретных 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

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

Общий результат выводится как интегральная оценка, складывающая из текущего контроля - 50% и промежуточного контроля - 50%.

Текущий контроль по дисциплине включает:

- ✓ - посещение занятий - 10 баллов,
- ✓ - участие на практических занятиях - до 100 баллов,
- ✓ - выполнение домашних (аудиторных) контрольных работ – до 100 баллов.

Промежуточный контроль по дисциплине включает:

- ✓ - устный опрос - до 100 баллов,
- ✓ - письменная контрольная работа - до 100 баллов,
- ✓ - тестирование – до 100 баллов.

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

а) адрес сайта курса

Moodle [Электронный ресурс]: система виртуального обучения: [база данных] / Даг. гос. ун-т. – г. Махачкала. – Доступ из сети ДГУ или, после регистрации из сети ун-та, из любой точки, имеющей выход в Интернет, http://edu.dgu.ru/course/view.php?id=3109

б)Основная литература.

1. А. А. Губенков, В. Б. Байбурин. Информационная безопасность. - Новый издательский дом, 2018 г. - 128 стр. - ISBN 5-9643-0091-X.
2. Башлы П.Н. Информационная безопасность / - Ростов на Дону: Феникс, 2019. - 253стр.
3. Курило А.П. «Обеспечение информационной безопасности бизнеса» М. БДЦ-Пресс, 2018.
4. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2018. — 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(01.09.2020)
6. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2018. — 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(01.09.2021)
8. Щербаков А. Ю., Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.:Книжный мир, 2019. — 352 с — ISBN 978-5-8041-0378-2.

в) Дополнительная литература

9. Бабаш, Александр Владимирович. Информационная безопасность : лаб. практикум; учеб. пособие / Бабаш, 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, 2020. - 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, 2018. - 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, 2016. - 544 с. - ISBN 5-93517-292-5 : 154-00.
14. 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(01.09.2021)
15. 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, 2017. - 263 с. - (Основы информационных технологий). - ISBN 5-9556-0053-1 : 176-00.
16. 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, 2016. - 335 с. - ISBN 5-94798-918-2 : 154-00.
17. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей : учеб.пособие для студентов - М. : ФОРУМ: ИНФРА-М, 2018. - 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 эксплоиты
- ✓ 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.

В процессе преподавания дисциплины предполагается использование современных технологий визуализации учебной информации (создание и демонстрация презентаций), использование ресурсов электронной информационно-образовательной среды университета, в том числе учебного курса «Информационная безопасность», который находится в процессе разработки для размещения на платформе Moodle ДГУ http://moodle.dgu.ru/ (автор-разработчик Арипова П.Г.).

Проведение данной дисциплины предполагает использование специального программного обеспечения:

MICROSOFT SQL SERVER 2016. MICROSOFT IMAGINE PREMIUM.Контракт № 188-ОА от 21 ноября 2018гс ООО «Софтекс».

WINDOWS 10. MICROSOFTIMAGINEPREMIUM.Контракт № 188-ОАот 21 ноября 2018гс ООО «Софтекс».

Используется также следующее лицензионное программное обеспечение общего назначения и информационные справочные системы:

MS Word, MS PowerPoint. Пакет офисных приложений OfficeStd 2016 RUS OLP NL Acdmc, Контракт №219-ОА от 19.12.2016 г. с ООО «Фирма АС».

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

Минимально необходимый для реализации ОПОП бакалавриатаперечень 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, оборудованные интерактивными, мультимедийными досками, проекторами, что позволяет читать лекции в формате презентаций, разработанных с помощью пакета прикладных программ, использовать наглядные, иллюстрированные материалы, обширную информацию в табличной и графической формах, пакет прикладных обучающих программ, а также электронные ресурсы сети Интернет.

Для проведения занятий по дисциплине необходимы учебные аудитории для проведения занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и

промежуточной аттестации с достаточным количеством посадочных мест. Учебные аудитории для проведения занятий лекционного типа должны быть оснащены современным демонстрационным (мультимедийным) оборудованием для показа презентаций. Помещения для самостоятельной работы обучающихся должны быть оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.

г. Махачкала, ул. Батырая, 2/12, № 405 - учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	**Специализированная мебель:** - количество посадочных мест - 64 ; - меловая доска - 1шт.; - стол преподавателя – 1 шт.; **Технические средства обучения:** - проектор; - экран ScreenMedia 200*200; - выход в интернет.
г. Махачкала, ул. Батырая, 2/12, № 411 - учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	**Специализированная мебель:** - количество посадочных мест - 30 ; - меловая доска - 1шт.; - маркерная доска - 1шт.; - стол преподавателя – 1 шт.; **Технические средства обучения:** - проектор BenQ MX661; - экран ScreenMedia 200*200; - выход в интернет.
г. Махачкала, ул. Батырая 2/12, № 434 (компьютерный класс) - учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации, самостоятельной работы обучающихся.	**Специализированная мебель:** - количество посадочных мест – 38; - меловая доска - 1 шт.; - стол преподавателя – 1 шт.; - кафедра – 1шт.; **Технические средства обучения:** -компьютеры AMD Athon II X3 445 BOX, Asus M4A88T-M, DDR-II 2Gb, HDD 500Gb - 10 шт.; - Pentium Dual-Core E2160, Asus P5B-VM SE, HDD SATA-II 80Gb, DVD+Rom – 17шт. - выход в интернет.