ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»

Утверждены решением
Ученого совета ДГУНХ,
Протокол №10
от 30 мая 2017г

КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

НАПРАВЛЕНИЕ ПОДГОТОВКИ – 09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА, ПРОФИЛЬ «ПРИКЛАДНАЯ ИНФОРМАТИКА В ЭКОНОМИКЕ»

Уровень высшего образования - бакалавриат

Махачкала – 2017

УДК 004.056.5
ББК 32.973.2

Составитель – Эмирбеков Эльдар Меликович, старший преподаватель кафедры «Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент - Якубов Амучи Загирович, кандидат физико-математических наук, доцент кафедры "Прикладная математика и информационные технологии" ДГУНХ

Внешний рецензент – Меджидов Зияудин Гаджиевич, кандидат физико-математических наук, старший научный сотрудник Отдела математики и информатики Дагестанского научного центра Российской Академии Наук

Представитель работодателя - Сайидахмедов Сайидахмед Сергеевич, генеральный директор компании «Текама».

*Оценочные материалы по дисциплине «*Информационная безопасность*» разработаны в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 «Прикладная информатика», утвержденного приказом Министерства образования и науки Российской Федерации от 12 марта 2015 г., № 207, в соответствии с приказом от 5 апреля 2017г., № 301 Министерства образования и науки РФ.*

Оценочные материалы по дисциплине «Информационная безопасность» размещены на официальном сайте www.dgunh.ru

Эмирбеков Э.М. Оценочные материалы по дисциплине «Информационная безопасность» для направления подготовки 09.03.03 Прикладная информатика, профиль «Прикладная информатика в экономике». – Махачкала: ДГУНХ, 2017 г., - 28 с.

Рекомендованы к утверждению Учебно-методическим советом ДГУНХ 29 мая 2017 г.

Рекомендованы к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 09.03.03 Прикладная информатика, профиль «Прикладная информатика в экономике», к.э.н., Раджабов К.Я.

Одобрены на заседании кафедры «Информационные технологии и информационная безопасность» 25 мая 2017 г., протокол № 10.

СОДЕРЖАНИЕ

Назначение оценочных материалов

Оценочные материалы для текущего контроля успеваемости (оценивания хода освоения дисциплин), для проведения промежуточной аттестации (оценивания промежуточных и окончательных результатов обучения по дисциплине) обучающихся по дисциплине «Информационная безопасность» на соответствие их учебных достижений поэтапным требованиям образовательной программы высшего образования 09.03.03 Прикладная информатика, профиль «Прикладная информатика в экономике».

Оценочные материалы по дисциплине «Информационная безопасность» включают в себя: перечень компетенций с указанием этапов их формирования в процессе освоения ОП ВО; описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания; типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения ОПОП; методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Оценочные материалы сформированы на основе ключевых принципов оценивания:

- валидности: объекты оценки должны соответствовать поставленным целям обучения;
- надежности: использование единообразных стандартов и критериев для оценивания достижений;
- объективности: разные обучающиеся должны иметь равные возможности для достижения успеха.

Основными параметрами и свойствами оценочных материалов являются:

- предметная направленность (соответствие предмету изучения конкретной дисциплины);
- содержание (состав и взаимосвязь структурных единиц, образующих содержание теоретической и практической составляющих дисциплины);
- объем (количественный состав оценочных материалов);
- качество оценочных материалов в целом, обеспечивающее получение объективных и достоверных результатов при проведении контроля с различными целями.
-

I.ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ЭТАПОВ ИХ ФОРМИРОВАНИЯ

1.1 Перечень формируемых компетенций

код компетенции	формулировка компетенции
ОПК	**ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ОПК-4	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК	**ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ПК-1	способностью проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе
ПК-18	способностью принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью

1.2. Перечень компетенций с указанием видов оценочных средств

Формируемые компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Уровни освоения компетенций	Критерии оценивания сформированности компетенций	Виды оценочных средств
ОПК-4 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной	– **Знать**: современные стандарты в области информационной безопасности	Пороговый уровень	Обучающийся слабо (частично) знает современные стандарты в области информационной безопасности	**Блок А –**задания репродуктивного уровня – тестовые задания
		Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает современные стандарты в области информационной безопасности	

безопасности		Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает современные стандарты в области информационной безопасности	
	Уметь: обосновывать организационно-технические мероприятия по защите информации в ИС	Пороговый уровень	Обучающийся слабо (частично) умеет обосновывать организационно-технические мероприятия по защите информации в ИС	**Блок В** – задания реконструктивного уровня – вопросы для обсуждения - практическая работа;
		Базовый уровень	Обучающийся с незначительными затруднениями умеет обосновывать организационно-технические мероприятия по защите информации в ИС	
		Продвинутый уровень	Обучающийся умеет использовать обосновывать организационно-технические мероприятия по защите информации в ИС	
	Владеть: навыками применения политики безопасности предприятия;	Пороговый уровень	Обучающийся слабо (частично) владеет навыками применения политики безопасности предприятия;	**Блок С** – задания практико-ориентированного уровня Лабораторная работа
		Базовый уровень	Обучающийся с небольшими затруднениями владеет навыками применения политики безопасности предприятия;	
		Продвинутый уровень	Обучающийся свободно владеет навыками применения политики безопасности предприятия;	
ПК-1. Способностью проводить обследование организаций, выявлять информационные потребности пользователей,	**Знать:** виды угроз ИС и методы обеспечения информационной безопасности	Пороговый уровень	Обучающийся слабо (частично) знает виды угроз ИС и методы обеспечения информационной безопасности	**Блок А –**задания репродуктивного уровня – тестовые задания
		Базовый уровень	Обучающийся с незначительными	

формировать требования к информационной системе			ошибками и отдельными пробелами знает виды угроз ИС и методы обеспечения информационной безопасности	
		Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает виды угроз ИС и методы обеспечения информационной безопасности	
	Уметь: выявлять угрозы информационной безопасности	Пороговый уровень	Обучающийся слабо (частично) умеет выявлять угрозы информационной безопасности	**Блок В** – задания реконструктивного уровня – вопросы для обсуждения практическая работа;
		Базовый уровень	Обучающийся с незначительными затруднениями умеет выявлять угрозы информационной безопасности	
		Продвинутый уровень	Обучающийся умеет выявлять угрозы информационной безопасности	
ПК-18 способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью	**Знать**: - организационно-правовые методы информационной безопасности	Пороговый уровень	Обучающийся слабо (частично) знает организационно-правовые методы информационной безопасности	**Блок А –**задания репродуктивного уровня – тестовые задания; – вопросы для обсуждения
		Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает организационно-правовые методы информационной безопасности	
		Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает организационно-правовые методы информационной безопасности	
	Уметь: применять программно-технические средства защиты	Пороговый уровень	Обучающийся слабо (частично) умеет применять программно-технические средства	**Блок В** – задания реконструктивного уровня – практическая работа

			защиты	
		Базовый уровень	Обучающийся с незначительными затруднениями умеет применять программно-технические средства защиты	
		Продвинутый уровень	Обучающийся умеет применять программно-технические средства защиты	
	Владеть: основными технологиями построения защищённых экономических информационных систем	Пороговый уровень	Обучающийся слабо (частично) владеет основными технологиями построения защищённых экономических информационных систем	**Блок С** – задания практико-ориентированного уровня Лабораторная работа
		Базовый уровень	Обучающийся с небольшими затруднениями владеет основными технологиями построения защищённых экономических информационных систем	
		Продвинутый уровень	Обучающийся свободно владеет основными технологиями построения защищённых экономических информационных систем;	

РАЗДЕЛ 2. Задания, необходимые для оценки планируемых результатов обучения по дисциплине

Для проверки сформированности компетенции ОПК-4 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Блок А. Задания репродуктивного уровня («знать»)

А.1 Фонд тестовых заданий по дисциплине

1. К субъектам информационной системы не относится …
   А. Владелец;
   Б. Пользователь;
   В. Регулятор;
   Г. Собственник;
2. Информационная система – это …
   А. набор программных и технических средств;
   Б. упорядоченную совокупность документов и информационных технологий, реализующих информационные процессы;
   В. упорядоченная совокупность документов, относящихся к определенной области;
   Г. набор программных средств, относящихся к одной задаче.
3. Несанкционированный доступ – это …
   А. доступ или воздействие с нарушением правил доступа;
   Б. изменение пароля с правами администратора;
   В. доступ в незащищенную систему пользователя;
   Г. изменение пароля доступа в систему пользователем.
4. К конфиденциальной информации не относится …
   А. служебная тайна;
   Б. персональные данные;
   В. государственная тайна;
   Г. коммерческая тайна.
5. Что не относится к непреднамеренным воздействиям?
   А. воздействия из-за ошибок пользователя;
   Б. сбой технических средств;
   В. сбой программных средств;
   Г. внедрение вируса в автоматическом режиме.
6. Целью защиты информации является …
   А. предотвращение экономического ущерба собственнику, владельцу или пользователю информации;
   Б. предотвращения доступа в информационную систему нелегитимным пользователям;
   В. недопущение распространения конфиденциальной информации;
   Г. соблюдение политики безопасности и выполнение правил хранения информации.
7. Что не является характеристикой информации?
   А. статичность;
   Б. тип доступа;
   В. время отклика;
   Г. стоимость создания.
8. Какая стоимостная характеристика информации совпадает с себестоимостью информации?

А. стоимость создания;
Б. стоимость потери конфиденциальности;
В. стоимость скрытого нарушения целостности;
Г. стоимость утраты.

9. Время жизни информации – это …
А. время, пока информация хранится в информационной системе;
Б. время, пока информация актуальна;
В. время, пока информация интересна для злоумышленников;
Г. время, пока стоимость создания информации выше стоимость потери.

10. Каков максимальный срок хранения документов с грифом "секретно"?
А. 5 лет;
Б. 10 лет;
В. неограничен;
Г. до тех пор, пока информация не будет скомпрометирована.

11. Что не относится к задачам информационной безопасности?
А. целостность и секретность;
Б. электронная подпись и датирование;
В. устойчивость связи и определение трафика;
Г. неотказуемость и анонимность.

12. Право на использование некоторого ресурса – это …
А. уполномочивание;
Б. контроль доступа;
В. право собственности;
Г. сертификация.

13. Какие методы реализуют контроль соблюдения установленного порядка к защищаемой информации?
А. правовые;
Б. административные;
В. технические;
Г. все перечисленные.

14. Какие методы не относятся к обеспечению информационной безопасности?
А. принуждение и побуждение;
Б. управление доступом и регламентация;
В. маскировка и препятствие;
Г. скрытый доступ и копирование сообщений.

15. Методами защиты с "черным ящиком" называют …
А. методы, не имеющие математического обоснования стойкости;
Б. "слепые" полуавтоматические методы;
В. криптографические методы;
Г. методы, реализованные на аппаратном уровне.

Блок В. Задания реконструктивного уровня («уметь»)

В.1 Вопросы для обсуждения

1. Определение информационной безопасности, угроз, уязвимости. Цели защиты.
2. Характеристики информации, применительно к задачам защиты. Физические и экономические характеристики. Взаимосвязь между стоимостями.
3. Информационная безопасность в условиях функционирования в России глобальных сетей.
4. Тенденции развития преступлений в сфере информационных технологий.
5. Internet как среда для компьютерных преступлений.
6. Основные задачи информационной безопасности.
7. Основные методы обеспечения защиты информационной системы. Законодательные, административные, технические. Классификация методов.
8. Ключевые свойства информации. Понятие угрозы. Секретность, конфиденциальность, доступность. Определение и классификация угроз.
9. Угроза нарушения конфиденциальности. Служебная и предметная информация. Непрерывность защиты.
10. Угроза нарушения целостности. Статическая и динамическая целостность. Примеры нарушений целостности.
11. Угроза отказа служб. Классификация угроз и методы минимизации последствий.

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С1. Лабораторная работа

Лабораторная работа № 1 «Сравнительный анализ понятийных аппаратов различных источников в области защиты информации».

Работа посвящена проведению сравнительного анализа понятийных аппаратов применяемых в различных источниках раскрывающих вопросы обеспечения защиты компьютерной информации.
Изучение основных терминов и определений в основных руководящих документах по защите информации.
В процессе выполнения работы студентам необходимо проанализировать различные литературные источники по вопросам защиты информации в том числе ГОСТы, ОСТы, РД ФСТЭК, книги, учебники, статьи , а используя материал, представленный в сети Интернет (на сайтах по безопасности информации (рекомендуется воспользоваться ссылкой http://www.glossary.ru)).

Глоссарий терминов (понятий) в области защиты информации (не менее 12 единиц) представить в печатной форме (формат А4) в соответствии с таблицей. Для каждого исследуемого термина должно быть указано не менее двух источников.

Понятие/термин	Источник 1	Источник 2	Сравнение	Примечание
	Определение	Определение		

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1.Перечень экзаменационных вопросов

1. Стоимостные характеристики информации и их соотношения.
2. Internet как среда для компьютерных преступлений.
3. Основные задачи информационной безопасности.
4. Основные методы обеспечения защиты информационной системы.
5. Определение и классификация угроз.
6. Потенциальные противники: классификация и характеристика.
7. Каналы утечки информации.
8. Классификация атак и их характеристики.
9. Сетевые атаки: основные виды.
10. Формулирование основных положений информационных положений.
11. Принципы обеспечения информационной безопасности.
12. Формальные модели доступа к данным.
13. Монитор безопасности и его функции.
14. Политика безопасности информационных систем
15. Таксономия нарушений информационной безопасности вычислительной системы.

Для проверки сформированности компетенции ПК-1 способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе

Блок А. Задания репродуктивного уровня («знать»)

А.1 Фонд тестовых заданий по дисциплине

Тесты типа А.

1. Что представляет собой ресурс системы защиты информации ?

А - количество специалистов по защите информации

В - состав инженерно-технических сооружений

С - выделенные денежные средства

Д – все вместе

2. Что надо определить перед выбором мер защиты информации ?

А – квалификацию персонала

В – угрозы безопасности информации

С – систему пожарно-охранной сигнализации

3. Локальные показатели эффективности защиты информации подразделяются на :

А – тактические и стратегические

В – оперативные и постоянные

С – функциональные и экономические

Д – территориальные и пространственные

4. Что означает принцип экономичности защиты информации?

А – минимизация затрат на защиту информации

В – затраты на защиту информации не должны превышать возможный ущерб от реализации угроз

С – численность службы защиты информации не должна превышать 7 чел.

Д – комплексное использование различных способов и средств защиты информации

5. Что означает принцип рациональности защиты информации?

А – использование только сертифицированных средств защиты

В – системный подход к инженерно—технической защите информации

С – минимизацию ресурсов на обеспечение необходимого уровня безопасности информации

Д – все вместе

6. Зоны защиты объектов информатизации бывают:

А - независимыми, пересекающимися и вложенными

В – автономными, многоярусными и многозвенными

С - укрепленными, локальными и общими

7. Чем отличаются ОТСС от ВТСС?

А – потребляемой мощностью

В – наличием принятых мер по защите информации
С – не могут использоваться для обработки открытой информации
Д – большей скоростью обработки информации

А2. Вопросы для обсуждения

1. Основные задачи инженерно-технической защиты информации. Факторы, влияющие на эффективность инженерно-технической защиты информации.
2. Базовые принципы инженерно-технической защиты информации (общие, специальные, дополнительные).
3. Объект информатизации (определение). Основные технические средства и системы (ОТСС). Вспомогательные технические средства и системы (ВТСС). Технический канал утечки информации (определение). Схема технического канала утечки информации
4. Показатели эффективности инженерно-технической защиты информации.
5. Основные направления инженерно-технической защиты информации (остановиться на информационном и энергетическом скрытии).

Блок В. Задания реконструктивного уровня («уметь»)

В1. Практическая работа

Практическая работа «Выбор объекта и определение информационных ресурсов»

При подготовки к занятию необходимо обратить внимание на следующие моменты.

1. Основные понятия и сущность информационных ресурсов.
2. Информационное описание объекта и формирование информационных ресурсов.
3. Классификация информационных ресурсов

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1.Перечень экзаменационных вопросов

1. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации.
2. Принципы защиты информации техническими средствами.
3. Основные направления инженерно-технической защиты информации.
4. Показатели эффективности инженерно-технической защиты информации.

5. Понятие об информации как предмете защиты. Основные свойства информации как предмета защиты.
6. Характеристики технических каналов утечки информации.
7. Физические принципы технических каналов передачи информации.

Для проверки сформированности компетенции ПК-18: Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью **предприятия**

Блок А. Задания репродуктивного уровня («знать»)

А.1 Фонд тестовых заданий по дисциплине

1. Основные угрозы доступности информации:
а)**непреднамеренные ошибки пользователей**
б)злонамеренное изменение данных
в)хакерская атака
г)**отказ программного и аппаратно обеспечения**
д)**разрушение или повреждение помещений**
е)перехват данных

2. Суть компрометации информации
а)внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации
б)несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений
в)**внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений**

3. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, ...
а)**с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой - ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды**
б)с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
в)способна противостоять только информационным угрозам, как внешним так и внутренним
г)способна противостоять только внешним информационным угрозам

4. Методы повышения достоверности входных данных
а)**Замена процесса ввода значения процессом выбора значения из предлагаемого множества**
б)Отказ от использования данных
в)Проведение комплекса регламентных работ
г)**Использование вместо ввода значения его считывание с машиночитаемого носителя**
д)**Введение избыточности в документ первоисточник**
е)**Многократный ввод данных и сличение введенных значений**

5. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)
а)**МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения**
б)МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты
в)МЭ работают только на сетевом уровне, а СОВ – еще и на физическом

6. Сервисы безопасности:
а)**идентификация и аутентификация**
б)**шифрование**
в)инверсия паролей
г)**контроль целостности**
д)регулирование конфликтов
е)**экранирование**
ж)**обеспечение безопасного восстановления**
з)кэширование записей

7. Под угрозой удаленного администрирования в компьютерной сети понимается угроза ...
а)**несанкционированного управления удаленным компьютером**
б)внедрения агрессивного программного кода в рамках активных объектов Web-страниц
в)перехвата или подмены данных на путях транспортировки
г)вмешательства в личную жизнь
д)поставки неприемлемого содержания

8. Причины возникновения ошибки в данных
а)**Погрешность измерений**
б)**Ошибка при записи результатов измерений в промежуточный документ**
в)Неверная интерпретация данных
г)**Ошибки при переносе данных с промежуточного документа в компьютер**
д)Использование недопустимых методов анализа данных
е)Неустранимые причины природного характера
ж)**Преднамеренное искажение данных**

з)**Ошибки при идентификации объекта или субъекта хозяйственной деятельности**

9. К формам защиты информации не относится...
а)**аналитическая**
б)правовая
в)организационно-техническая
г)**страховая**

10. Наиболее эффективное средство для защиты от сетевых атак
а)**использование сетевых экранов или "firewall"**
б)использование антивирусных программ
в)посещение только "надёжных" Интернет-узлов
г)использование только сертифицированных программ-броузеров при доступе к сети Интернет

11. Информация, составляющая государственную тайну не может иметь гриф...
а)**"для служебного пользования"**
б)"секретно"
в)"совершенно секретно"
г)"особой важности"

12. Разделы современной криптографии:
а)**Симметричные криптосистемы**
б)**Криптосистемы с открытым ключом**
в)Криптосистемы с дублированием защиты
г)**Системы электронной подписи**
д)Управление паролями
е)Управление передачей данных
ж)**Управление ключами**

13. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности рекомендации X.800
а)**Оранжевая книга**
б)Закон "Об информации, информационных технологиях и о защите информации"

14. Утечка информации – это ...
а)**несанкционированный процесс переноса информации от источника к злоумышленнику**
б)процесс раскрытия секретной информации
в)процесс уничтожения информации
г)непреднамеренная утрата носителя информации

15. Основные угрозы конфиденциальности информации:
а)**маскарад**
б)карнавал
в)переадресовка
г)**перехват данных**
д)блокирование
е)**злоупотребления полномочиями**

Блок В. Задания реконструктивного уровня («уметь»)

В.1 Вопросы для обсуждения

1. Виды противников или "нарушителей".
2. Виды и каналы утечки информации. Непосредственные и косвенные каналы. Каналы, предполагающие изменение структуры информационной структуры.
3. Классификация атак.
4. Сетевые атаки.
5. Подходы к обеспечению информационной безопасности. Формулирование основных положений информационных положений.
6. Принципы обеспечения информационной безопасности. Системность, комплексность, непрерывность, разумная достаточность, гибкость, открытость алгоритмов, простота применения.
7. Административный уровень защиты информации.
8. Разделение политики безопасности по уровням. Описание функций административного уровня безопасности.
9. Разработка и реализация политики безопасности.
10. Функции политики безопасности по уровням. Вопросы, решаемые при разработке политики безопасности.

В 2. Практическая работа

Практическая работа № 1 «Изучение методов комплексного исследование объекта информатизации»

Цель работы: изучить положительные и отрицательные стороны проведения обследования защищенности объекта информатизации (ОИ) посредством существующих стандартов и методик.

Практиуческая работа№2 «Изучение построения системы защиты информации на основе нормативных актов и методических указаний»

Цель работы: изучить перечень нормативных документов на основе которых осуществляется построение системы защиты информации.

Блок С. Задания практикоориентированного уровня для диагностирования сформированности компетенций («владеть»)

С1. Лабораторная работа

Лабораторная работа №1 «Изучение действующей нормативной документации объекта информатизации»

Цель работы: изучить действующую нормативную документацию объекта информатизации.

Задание:

- Составить перечень внутренних нормативных документов предприятия регламентирующих защиту информацию.
- Провести сравнение имеющегося перечня нормативных документов с необходимым.
- Написать один из внутренних документов, которые отсутствует на объекте информатизации.

Лабораторная работа №2 «Составление плана мероприятий по улучшению защищённости объекта информатизации»

Цель работы: изучить методику составления плана мероприятий по улучшению защищённости объекта информатизации.

Задание:

Составить план мероприятий по улучшению информационной безопасности

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1.Перечень экзаменационных вопросов

1. Уровни правового обеспечения информационной безопасности.
2. Доктрина информационной безопасности России.
3. Задачи и методы криптографии.
4. Основные криптографические протоколы.
5. Основные аппаратные средства защиты.
6. Основные программные средства защиты.
7. Основные методы идентификации и аутентификации.
8. Сервисы управления доступом.
9. Протоколирование и аудит. Задачи аудита.

10. Основы защиты Internet-подключений.

11. Вирусы. Виды вирусов.

12. Антивирусное программное обеспечение.

13. Стандарты обеспечения информационной безопасности.

14. Общие принципы построения защищенных систем.

РАЗДЕЛ 3.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Балльно-рейтинговая система является базовой системой оценивания сформированности компетенций обучающихся очной формы обучения.

Итоговая оценка сформированности компетенции(й) обучающихся в рамках балльно-рейтинговой системы осуществляется в ходе текущего контроля успеваемости, промежуточной аттестации и определяется как сумма баллов, полученных обучающимися в результате прохождения всех форм контроля.

Оценка сформированности компетенции(й) по дисциплине складывается из двух составляющих:

✓ первая составляющая – оценка преподавателем сформированности компетенции(й) в течение семестра в ходе текущего контроля успеваемости (максимум 100 баллов). Структура первой составляющей определяется технологической картой дисциплины, которая в начале семестра доводится до сведения обучающихся;

✓ вторая составляющая – оценка сформированности компетенции(й) обучающихся на экзамене (максимум – 30 баллов).

уровни освоения компетенций	продвинутый уровень	базовый уровень	пороговый уровень	допороговый уровень
100 – балльная шкала	85 и ≥	70 – 84	51 – 69	0 – 50
4 – балльная шкала	«отлично»	«хорошо»	«удовлетворительно»	«неудовлетворительно»

Шкала оценок при текущем контроле успеваемости по различным показателям

Показатели оценивания сформированности компетенций	***Баллы***	***Оценка***
Выполнение практических работ	0-10	«неудовлетворительно»

		«удовлетворительно» «хорошо» «отлично»
Проведение устного опроса	0-10	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Тестирование	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение лабораторных работ	0-20	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

Соответствие критериев оценивания уровню освоения компетенций по текущему контролю успеваемости

Баллы	***Оценка***	***Уровень освоения компетенций***	***Критерии оценивания***
0-50	«неудовлетворительно»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины
51-69	«удовлетворительно»	Пороговый уровень	Не менее 50% заданий, подлежащих текущему контролю успеваемости, выполнены без существенных ошибок
70-84	«хорошо»	Базовый уровень	Обучающимся выполнено не менее 75% заданий, подлежащих текущему контролю успеваемости, или при выполнении всех заданий допущены незначительные ошибки; обучающийся показал владение навыками систематизации материала и применения его при решении практических заданий; задания выполнены без ошибок
85-100	«отлично»	Продвинутый уровень	100% заданий, подлежащих текущему контролю успеваемости, выполнены самостоятельно и в требуемом объеме; обучающийся проявляет умение

			обобщать, систематизировать материал и применять его при решении практических заданий; задания выполнены с подробными пояснениями и аргументированными выводами

Шкала оценок по промежуточной аттестации

Наименование формы промежуточной аттестации	***Баллы***	***Оценка***
Экзамен	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»

Соответствие критериев оценивания уровню освоения компетенций по промежуточной аттестации обучающихся

Баллы	***Оценка***	***Уровень освоения компетенций***	***Критерии оценивания***
0-9	«неудовлетворительно»	Допороговый уровень	Обучающийся не приобрел знания, умения и не владеет компетенциями в объеме, закрепленном рабочей программой дисциплины; обучающийся не смог ответить на вопросы
10-16	«удовлетворительно»	Пороговый уровень	Обучающийся дал неполные ответы на вопросы, с недостаточной аргументацией, практические задания выполнены не полностью, компетенции, осваиваемые в процессе изучения дисциплины сформированы не в полном объеме.
17-23	«хорошо»	Базовый уровень	Обучающийся в целом приобрел знания и умения в рамках осваиваемых в процессе обучения по дисциплине компетенций; обучающийся ответил на все вопросы, точно дал определения и понятия, но затрудняется подтвердить теоретические положения

			практическими примерами; обучающийся показал хорошие знания по предмету, владение навыками систематизации материала и полностью выполнил практические задания
25-30	«отлично»	Продвинутый уровень	Обучающийся приобрел знания, умения и навыки в полном объеме, закрепленном рабочей программой дисциплины; терминологический аппарат использован правильно; ответы полные, обстоятельные, аргументированные, подтверждены конкретными примерами; обучающийся проявляет умение обобщать, систематизировать материал и выполняет практические задания с подробными пояснениями и аргументированными выводами

РАЗДЕЛ 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующие этапы формирования компетенций

Тестирование проводится с помощью системы дистанционного обучения «Прометей», входящей в состав электронной информационно-образовательной среды Дагестанского государственного университета народного хозяйства.

На тестирование отводится 45 минут. Каждый вариант тестовых заданий включает 30 вопросов.

Методика оценивания выполнения тестов

Баллы	***Оценка***	***Показатели***	***Критерии***
25-30	«отлично»	1. Полнота выполнения тестовых заданий; 2. Своевременность выполнения; 3. Правильность ответов на вопросы; 4. Самостоятельность тестирования; 5. и т.д.	Выполнено более 85 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос
19-24	«хорошо»		Выполнено более 70 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос; однако

			были допущены неточности в определении понятий, терминов и др.
6-18	«удовлетворительно»		Выполнено более 54 % заданий предложенного теста, в заданиях открытого типа дан неполный ответ на поставленный вопрос, в ответе не присутствуют доказательные примеры, текст со стилистическими и орфографическими ошибками.
0-5	«неудовлетвори-тельно»		Выполнено не более 53 % заданий предложенного теста, на поставленные вопросы ответ отсутствует или неполный, допущены существенные ошибки в теоретическом материале (терминах, понятиях).

Устный опрос проводится в первые 15 минут занятий семинарского типа в формате обсуждения с названными преподавателем студентами. Остальные обучающиеся вправе дополнить или уточнить ответ по своему желанию (соблюдаю очередность ответа). Основной темой для опроса являются вопросы для обсуждения, соответствующие теме предыдущей лекции, но преподаватель может уточнять задаваемый вопрос, задавать наводящие вопросы или сужать вопрос до отдельного аспекта обсуждаемой темы.

Методика оценивания ответов на устные вопросы

Баллы	***Оценка***	**Показатели**	**Критерии**
8-10	«отлично»	1. Полнота данных ответов; 2. Аргументированность данных ответов; 3. Правильность ответов на вопросы; 4. и т.д.	Полно и аргументировано даны ответы по содержанию задания. Обнаружено понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные. Изложение материала последовательно и правильно.

6-7	«хорошо»		Студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет.
3-5	«удовлетворительно»		Студент обнаруживает знание и понимание основных положений данного задания, но: 1) излагает материал неполно и допускает неточности в определении понятий или формулировке правил; 2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 3) излагает материал непоследовательно и допускает ошибки.
0-2	«неудовлетвори-тельно»		Студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал; отмечаются такие недостатки в подготовке студента, которые являются серьезным препятствием к успешному овладению последующим материалом.

Лабораторные работы выполняются в специализированной аудитории. Предусмотрено выполнение одной лабораторной работы в течение одного занятия согласно текущей тематике. Студенты должны выполнять задание самостоятельно, но имеют возможность обратиться к преподавателю за разъяснениями постановки задачи или оценкой правильности полученного результата. Если преподаватель вынужден разъяснять аспекты непосредственного выполнения шагов практической работы, то это негативно отражается на оценке выполняющего задание студента.

Методика оценивания выполнения лабораторных работ

Баллы	***Оценка***	Показатели	Критерии

17-20	«отлично»	1. Полнота выполнения практической/лабораторной работы; 2. Своевременность выполнения задания; 3. Последовательность и рациональность выполнения задания; 4. Самостоятельность решения; 5. и т.д.	Выполнены все задания практической/лабораторной работы, студент четко и без ошибок ответил на все контрольные вопросы
12-16	«хорошо»		Выполнены все задания практической/лабораторной работы; студент ответил на все контрольные вопросы с замечаниями
6-9	«удовлетворительно»		Выполнены все задания практической/ лабораторной работы с замечаниями; студент ответил на все контрольные вопросы с замечаниями.
0-5	«неудовлетвори-тельно»		Задание не выполнено

Методика оценивания выполнения практических работ

Баллы	***Оценка***	Показатели	Критерии
8-10	«отлично»	6. Полнота выполнения практической/лабораторной работы; 7. Своевременность выполнения задания; 8. Последовательность и рациональность выполнения задания; 9. Самостоятельность решения; 10. и т.д.	Выполнены все задания практической/лабораторной работы, студент четко и без ошибок ответил на все контрольные вопросы
6-7	«хорошо»		Выполнены все задания практической/лабораторной работы; студент ответил на все контрольные вопросы с замечаниями
3-5	«удовлетворительно»		Выполнены все задания практической/ лабораторной работы с замечаниями; студент ответил на все контрольные вопросы с замечаниями.
0-2	«неудовлетвори-тельно»		Задание не выполнено

Процедура промежуточной аттестации проходит в соответствии с Положением о промежуточной аттестации знаний студентов и учащихся ДГУНХ.

Аттестационные испытания проводятся преподавателем, ведущим лекционные занятия по данной дисциплине, или преподавателями, ведущими практические и лабораторные занятия (кроме устного экзамена). Присутствие посторонних лиц в ходе проведения аттестационных испытаний без разрешения ректора или проректора по учебной работе не допускается (за исключением работников университета, выполняющих контролирующие функции в соответствии со своими должностными обязанностями). В случае отсутствия ведущего преподавателя аттестационные испытания проводятся преподавателем, назначенным письменным распоряжением по кафедре (структурному подразделению).

Инвалиды и лица с ограниченными возможностями здоровья, имеющие нарушения опорно-двигательного аппарата, допускаются на аттестационные испытания в сопровождении ассистентов-сопровождающих.

Во время аттестационных испытаний обучающиеся могут пользоваться программой дисциплины, а также с разрешения преподавателя справочной и нормативной литературой, непрограммируемыми калькуляторами.

Лист актуализации оценочных материалов по дисциплине «Информационная безопасность»

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «22» мая 2018 г. № 10

Зав. кафедрой _____ Галяев В.С.

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «30» мая 2019 г. № 10

Зав. кафедрой _____ Галяев В.С.

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «30» июня 2020 г. № 12

Зав. кафедрой _____ Галяев В.С.

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

Протокол от «____» _____ 20___ г. №_____

Зав. кафедрой _____