ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»

Утверждены решением
Ученого совета ДГУНХ,
протокол № 11
от 06 июня 2023 г

КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

НАПРАВЛЕНИЕ ПОДГОТОВКИ
38.03.05 БИЗНЕС-ИНФОРМАТИКА, ПРОФИЛЬ
«МЕНЕДЖМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЭЛЕКТРОННЫЙ БИЗНЕС»

Уровень высшего образования - бакалавриат

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0D8142F19CA901112FC315F43B93C341
Владелец: Бучаев Ахмед Гамидович
Действителен: с 19.05.2022 до 12.08.2023

Махачкала – 2023

УДК 004.056.5
ББК 32.973.2

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

Внутренний рецензент - Гасанова Зарема Ахмедовна, кандидат педагогических наук, доцент кафедры «Информационные технологии и информационная безопасность» 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 - Ботвин Тимур Анатольевич, руководитель международных запусков Яндекс.Маркет ООО «Яндекс.Маркет».

Оценочные материалы по дисциплине «Информационная безопасность» разработаны в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 38.03.05 Бизнес-информатика, утвержденного приказом Министерства образования и науки Российской Федерации от 29 июля 2021 г., № 838, в соответствии с приказом Министерства науки и высшего образования Российской Федерации от 6.04.2021 г. № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»

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 38.03.05 Бизнес-информатика, профиль «Менеджмент информационных технологий и электронный бизнес». – Махачкала: ДГУНХ, 2023 г.– 28 с.

Рекомендованы к утверждению Учебно-методическим советом ДГУНХ 05 июня 2023 г.

Рекомендованы к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 38.03.05 Бизнес-информатика, профиль «Менеджмент информационных технологий и электронный бизнес», к.пед.н., Гасановой З.А.

Одобрены на заседании кафедры «Информационные технологии и информационная безопасность» 31 мая 2023 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 по направлению подготовки 38.03.05 Бизнес-информатика, профиль «Менеджмент информационных технологий и электронный бизнес».

Оценочные материалы по дисциплине «Информационная безопасность» включают в себя: перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины; 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.

РАЗДЕЛ 1. Перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины

1.1 Перечень формируемых компетенций

код компетенции	формулировка компетенции
ПК	**ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ПК-4	Способен разрабатывать и реализовывать проекты совершенствования ИТ-инфраструктуры предприятия для достижения стратегических целей и поддержки бизнес-процессов с учетом требований информационной безопасности

1.2. Перечень компетенций с указанием видов оценочных средств

Формируемые компетенции	***Код и наименование индикатора достижения компетенции***	***Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций***	***Уровни освоения компетенций***	***Критерии оценивания сформированности компетенций***	***Виды оценочных средств***
ПК-4. Способен разрабатывать и реализовывать проекты совершенствования ИТ-инфраструктуры предприятия для достижения стратегических целей и поддержки бизнес-	ИПК-4.2. Управляет информационной безопасностью предприятия	**Знать:** – - основные информационно-коммуникационные технологии и основные требования информационной безопасности; - виды угроз ИС и методы обеспечения информационной безопасности	Пороговый уровень	Обучающийся частично знает основные информационно-коммуникационные технологии и основные требования информационной безопасности, виды угроз ИС и методы обеспечения информационной безопасности	**Блок А –** задания репродуктивного уровня – тестовые задания; – вопросы для обсуждения.
			Базовый уровень	Обучающийся знает с незначительными ошибками и отдельными пробелами знает	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
процессов с учетом требований информационной безопасности				основные информационно-коммуникационные технологии и основные требования информационной безопасности, виды угроз ИС и методы обеспечения информационной безопасности	
			Продвинутый уровень	Обучающийся знает с требуемой степенью знает основные информационно-коммуникационные технологии и основные требования информационной безопасности, виды угроз ИС и методы обеспечения информационной безопасности	
		Уметь: − решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности; - выявлять угрозы информационной безопасности;	Пороговый уровень	Обучающийся частично умеет решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности, выявлять угрозы информационной безопасности	**Блок В** – задания реконструктивного уровня лабораторная работа.
			Базовый уровень	Обучающийся умеет с	

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
				незначительными затруднениями умеет решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности, выявлять угрозы информационной безопасности	
			Продвинутый уровень	Обучающийся умеет решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности, выявлять угрозы информационной безопасности	
		<u>Владеть:</u> – - культурой применения информационно-коммуникационных технологий с учетом основных требований информационной безопасности; - основными технологиями построения	Пороговый уровень	Обучающийся частично владеет культурой применения информационно-коммуникационных технологий с учетом основных требований информационной безопасности, основными технологиями построения защищённых	**Блок С** – задания практико - ориентированного уровня – деловая игра.

Формируемые компетенции	*Код и наименование индикатора достижения компетенции*	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Уровни освоения компетенций*	*Критерии оценивания сформированности компетенций*	*Виды оценочных средств*
		защищённых экономических информационных систем.		экономических информационных систем.	
			Базовый уровень	Обучающийся владеет культурой применения информационно-коммуникационных технологий с учетом основных требований информационной безопасности, основными технологиями построения защищённых экономических информационных систем.	
			Продвинутый уровень	Обучающийся свободно владеет культурой применения информационно-коммуникационных технологий с учетом основных требований информационной безопасности, основными технологиями построения защищённых экономических информационных систем.	

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

Для проверки сформированности компетенции ПК-4. Способен разрабатывать и реализовывать проекты совершенствования ИТ-инфраструктуры предприятия для достижения стратегических целей и поддержки бизнес-процессов с учетом требований информационной безопасности

ИПК-4.2. Управляет информационной безопасностью предприятия

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.
16. 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
17. 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**
18. 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
19. 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**

20. 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

21. 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

22. 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

23. 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**

24. К формам защиты информации не относится...

а)**аналитическая**

б)правовая

в)организационно-техническая
г)**страховая**

25. 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

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

27. 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**

28. 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"

29. 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

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

А2. 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.
12. Виды противников или "нарушителей".
13. Виды и каналы утечки информации. Непосредственные и косвенные каналы. Каналы, предполагающие изменение структуры информационной структуры.
14. Классификация атак.
15. Сетевые атаки.
16. Подходы к обеспечению информационной безопасности. Формулирование основных положений информационных положений.
17. Принципы обеспечения информационной безопасности. Системность, комплексность, непрерывность, разумная достаточность, гибкость, открытость алгоритмов, простота применения.
18. Административный уровень защиты информации.
19. Разделение политики безопасности по уровням. Описание функций административного уровня безопасности.
20. Разработка и реализация политики безопасности.

Функции политики безопасности по уровням. Вопросы, решаемые при разработке политики безопасности.

Блок В. Задания реконструктивного уровня («уметь»)

В2. Лабораторная работа

Лабораторная 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.

Лабораторная 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.

Лабораторная работа № 3 « 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 № 4 «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

Лабораторная работа № 5 «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		

Лабораторная работа №6 «Изучение содержания и последовательности работ по защите информации»

Цель работы: изучить содержание и последовательность работ выполняемых при построении комплексной системы защиты информации.

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

С1. Деловая игра

«Построение модели угроз информационной безопасности для малого предприятия»

Цель деловой игры: Анализ эффективности системы информационной безопасности (ИБ) организации с использованием аппарата моделирования с полным перекрытием множества угроз (программный инструментарий прилагается) с привлечением Специалистов отдела ИТ, Специалистов отдела защиты информации и Экспертов-аналитиков по ИБ.

Роли участников игры:

Специалисты отдела ИТ (3-4 человека)

При проектировании или оценки эффективности существующей системы защиты информации, чрезвычайно важно, чтобы различные конфликтные ситуации между сотрудниками службы ИТ и специалистами отдела защиты информации разрешались в форме продуктивного диалога.

Задачи специалистов отдела ИТ в данной деловой игре.

1. Подготовить для специалистов отдела защиты информации материалы по потенциальным угрозам ИБ, перечню инцидентов ИБ и прочиематериалы, необходимые для анализа и построения модели ИБ в организации. Для достижения поставленной цели специалисты отдела ИТ должны проанализировать структуру объекта оценки и подготовить ответы на вопросы для специалистов отдела защиты информации и экспертов-аналитиков.

2. Провести совместное совещание со специалистами отдела защиты информации (ЗИ) с целью анализа ответов на вопросы иформирования полного множества угроз; множества объектов защиты; множества средств защиты информации, имеющихся в данной организации.
3. Принять участие в итоговом совещании всех специалистов с целью анализа эффективности существующей системы защиты информации в организации и выработке рекомендаций по ее усовершенствованию.

Специалисты отдела защиты информации(3-4 человека)

Одной из задач специалистов по защите информации является оценка эффективности существующей в организации системы ИБ. Для решения этой задачи необходимо проводить интервью со специалистами ИТ с целью выявления слабостей в системе защиты информации, анализа инцидентов ИБ и подготовки материалов для построения модели: *угрозы-средства защиты-объекты оценки*.

Задачи специалистов отдела ЗИ в данной деловой игре.

1. Запросить у специалистов ИТ опросники, помочь в заполнении опросников и проконсультировать ИТ-специалистов в случае возникновения неоднозначных ситуаций.
2. Проанализировать полученные из отдела ИТ опросники (внести дополнительные сведения, при необходимости). На основании изучения описания организации и опросника, полученного от специалистов ИТ, заполнить формы анализа угроз ИБ для передачи экспертам-аналитикам.
3. Провести совместное совещание со специалистами отдела ИТ с целью формирования множества угроз; множества объектов защиты; множества средств защиты информации, имеющихся в данной организации.
4. Передать скорректированные тексты экспертам-аналитикам и внести сведения в базу данных.
5. Принять участие в итоговом совещании всех специалистов с целью анализа эффективности существующей системы защиты информации в организации и выработке рекомендаций по ее усовершенствованию.

Эксперты-аналитики в области ИБ (2 человека)

Сведения по множествам угроз безопасности; объектам оценки и средствам защиты информации на предприятии поступают к экспертам-аналитикам в области ИБ с целью их анализа, корректировки, построения модели угрозы-средства защиты-объекты защиты и анализу полученной модели.

Задачи экспертов-аналитиков в области ИБ в данной деловой игре.

1. Изучить инструкцию пользователя по работе с программным обеспечением для построения модели с полным перекрытием множества угроз и подготовить программу к использованию.
2. Проанализировав сведения, внесенные в базу данных специалистами ЗИ, скорректировать данные (после проведения совместного совещания со специалистами ИТ и ЗИ).

3. Построить модель с полным перекрытием множества угроз ИБ (описание работы с программным обеспечением)
4. Проанализировать полученную модель и сделать выводы по повышению эффективности системы ИБ в организации.
5. Собрать итоговое совещание со специалистами ИТ и ЗИ, где огласить выводы и обсудить дальнейшие мероприятия по повышению эффективности системы защиты информации в рассматриваемой организации.

Подведение итогов, подробный анализ деловой игры:

- общая оценка игры, подробный анализ реализации целей и задач, удачные и слабые стороны, их причины (проводится преподавателем);
- самооценка участниками исполнения полученных заданий, степень личной удовлетворенности (оценки сотрудникам службы ИТ и ЗИ выставляют руководители этих служб, назначенные перед началом игры; оценка деятельности экспертов по ИБ проводится преподавателем);
- характеристика профессиональных знаний и умений, выявленных в процессе игры (проводится преподавателем);

Критерием оценок может служить количество и содержательность выдвинутых идей (предложений), степень самостоятельности суждений, их практическая значимость. Оценивание осуществляется по десяти бальной шкале.

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.
16. Уровни правового обеспечения информационной безопасности.
17. Доктрина информационной безопасности России.

18. Задачи и методы криптографии.
19. Основные криптографические протоколы.
20. Основные аппаратные средства защиты.
21. Основные программные средства защиты.
22. Основные методы идентификации и аутентификации.
23. Сервисы управления доступом.
24. Протоколирование и аудит. Задачи аудита.
25. Основы защиты Internet-подключений.
26. Вирусы. Виды вирусов.
27. Антивирусное программное обеспечение.
28. Стандарты обеспечения информационной безопасности.
29. 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 лабораторных работ	0-20	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Проведение устного опроса	0-10	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Тестирование	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Проведение деловой игры	0-10	«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;	Выполнено более 85 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на

		3. Правильность ответов на вопросы; 4. Самостоятельность тестирования; 5. и т.д.	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.
15-18	«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.
0-14	«неудовлетворительно»		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**
9-10	«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.
7-8	«хорошо»		Студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет.
5-6	«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.
0-4	«неудовлетворительно»		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 во время лабораторных занятий. 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 лабораторной работы, то это негативно отражается на оценке выполняющего задание студента.

Методика оценивания выполнения лабораторных работ

Баллы	***Оценка***	Показатели	Критерии
18-20	«отлично»	1. Полнота выполнения лабораторной работы; 2. Своевременность выполнения задания; 3. Последовательность и рациональность выполнения задания; 4. Самостоятельность решения; 5. и т.д.	Выполнены все задания лабораторной работы, студент четко и без ошибок ответил на все контрольные вопросы
14-17	«хорошо»		Выполнены все задания лабораторной работы; студент ответил на все контрольные вопросы с замечаниями
10-13	«удовлетворительно»		Выполнены все задания лабораторной работы с замечаниями; студент ответил на все контрольные вопросы с замечаниями.
0-9	«неудовлетвори-тельно»		Задание не выполнено

Оценивание действий участников производиться по контролю качества принятых решений с позиции требований профессиональной деятельности и норм, а также раскрытия игрового план учебной деятельности. Деловая игра имеет свою структуру, в некоторых случаях структура различна, но как правило присутствуют обязательные общие этапы, такие, как: имитационная модель, игровая модель, цели игры, сценарий, распределение ролей, правила игры и подведение итогов.

Методика оценивания участников деловой игры

Баллы	***Оценка***	**Показатели**	**Критерии**
8-10	«отлично»	1. Полнота достижения цели; 2. Своевременность выполнения; 3. Правильность ответов на вопросы; 4. и т.д.	Основные требования к решению учебных и профессионально-ориентированных задач путем игрового моделирования реальной проблемной ситуации выполнены. Продемонстрировано умение анализировать и решать типичные профессиональные задачи

6-7	«хорошо»		Основные требования к решению учебных и профессионально-ориентированных задач деловой игры выполнены, но при этом допущены недочеты. В частности, недостаточно раскрыты навыки критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки, креативности, нестандартности предлагаемых решений
3-5	«удовлетворительно»		Имеются существенные отступления от достижения поставленной цели деловой игры. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат
0-2	«неудовлетвори-тельно»		Задача деловой игры не раскрыта, обнаруживается существенное непонимание проблемы

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 «_____»_____ 20___ г. №_____

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

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

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

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

Зав. кафедрой _____

Оценочные материалы пересмотрены,
обсуждены и одобрены на заседании кафедры

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

Зав. кафедрой _____