ГАОУ ВО «ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА»

Утверждены решением
Ученого совета ДГУНХ,
протокол № 9
от 24 марта 2025 г.

КАФЕДРА «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ПО ДИСЦИПЛИНЕ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

НАПРАВЛЕНИЕ ПОДГОТОВКИ 10.03.01
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПРОФИЛЬ
«БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

Уровень высшего образования - бакалавриат

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00C5A9FA0FAD6D6153888A98846B419FD3
Владелец: Бучаев Ахмед Гамидович
Действителен: с 11.07.2024 до 04.10.2025

Махачкала – 2025

УДК 681.518(075.8)
ББК 32.81.73

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

Внутренний рецензент – Галяев Владимир Сергеевич, кандидат физико-математических 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 - Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза», эксперт-представитель работодателя.

Оценочные материалы по дисциплине «Основы информационной безопасности» разработаны в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 17 ноября 2020 г., № 1427, 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 «Основы информационной безопасности» размещены на официальном сайте www.dgunh.ru

Эмирбеков Э.М. Оценочные материалы по дисциплине «Основы информационной безопасности» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2025 г. – 32 с.

Рекомендованы к утверждению Учебно-методическим советом ДГУНХ 10 марта 2025 г.

Рекомендованы к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

Одобрены на заседании кафедры «Информационные технологии и информационная безопасность» 24 февраля 2025 г., протокол № 7.

.

СОДЕРЖАНИЕ

Назначение оценочных материалов……..4

РАЗДЕЛ 1. Перечень компетенций с указанием видов оценочных средств в процессе освоения дисциплины ..…….……5

1.1 Перечень формируемых компетенций……5

1.2 Перечень компетенций с указанием этапов их формирования…….5

РАЗДЕЛ 2. Задания, необходимые для оценки планируемых результатов обучения по дисциплине……12

РАЗДЕЛ 3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания……..23

РАЗДЕЛ 4.Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующие этапы формирования компетенций…….26

Лист актуализации оценочных материалов по дисциплине…….…32

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 «Основы информационной безопасности» на соответствие их учебных достижений поэтапным требованиям образовательной программы высшего образования 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем»

Оценочные материалы по дисциплине «Основы информационной безопасности» 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
ОПК	**ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности

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***
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и	ИОПК-1.1 Использует основные понятия и определения в области информационных технологий и информационной безопасности	**<u>Знать:</u>** - цели, задачи, принципы и основные направления обеспечения информационной безопасности	Пороговый уровень	Обучающийся слабо (частично) знает цели, задачи, принципы и основные направления обеспечения информационной безопасности	**Блок А** **–**задания репродуктивного уровня – вопросы для обсуждения - тестовые задания
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает цели, задачи, принципы и	

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*
государства				основные направления обеспечения информационной безопасности	
			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает цели, задачи, принципы и основные направления обеспечения информационной безопасности	
		<u>Уметь:</u> **-** определять ресурсы и информацию подлежащие защите	Пороговый уровень	Обучающийся слабо (частично) умеет определять ресурсы и информацию подлежащие защите	**Блок В** – задания реконструктивного уровня – тематика рефератов и презентаций
			Базовый уровень	Обучающийся с незначительными затруднениями умеет определять ресурсы и информацию подлежащие защите	
			Продвинутый уровень	Обучающийся умеет определять ресурсы и информацию подлежащие защите	

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*
		Владеть: - методами формирования требований по защите информации	Пороговый уровень	Обучающийся слабо (частично) владеет методами формирования требований по защите информации	**Блок С** – задания практико-ориентированного уровня – практическая работа
			Базовый уровень	Обучающийся с небольшими затруднениями владеет методами формирования требований по защите информации	
			Продвинутый уровень	Обучающийся свободно владеет методами формирования требований по защите информации	
	ИОПК-1.2. Классифицирует и оценивает угрозы информационной безопасности	**Знать:** - угрозы информационной безопасности	Пороговый уровень	Обучающийся слабо (частично) знает угрозы информационной безопасности	**Блок А** **–**задания репродуктивного уровня – вопросы для обсуждения
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает угрозы информационной безопасности	
			Продвинутый уровень	Обучающийся с требуемой степенью	

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*
				полноты и точности знает угрозы информационной безопасности	
		<u>Уметь:</u> **-** классифицировать и оценивать угрозы информационной безопасности	Пороговый уровень	Обучающийся слабо (частично) умеет классифицировать и оценивать угрозы информационной безопасности	**Блок В** – задания реконструктивного уровня – тематика рефератов и презентаций
			Базовый уровень	Обучающийся с незначительными затруднениями умеет классифицировать и оценивать угрозы информационной безопасности	
			Продвинутый уровень	Обучающийся умеет классифицировать и оценивать угрозы информационной безопасности	
		<u>Владеть:</u> - навыками определения угроз информационной безопасности	Пороговый уровень	Обучающийся слабо (частично) владеет навыками определения угроз информационной безопасности	**Блок С** – задания практико-ориентированного уровня – практическая работа
			Базовый уровень	Обучающийся с небольшими затруднениями	

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*
				владеет навыками определения угроз информационной безопасности	
			Продвинутый уровень	Обучающийся свободно владеет навыками определения угроз информационной безопасности	
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ИОПК-8.1. Анализирует научно-техническую литературу, нормативные и методические документы в целях решения задач профессиональной деятельности	**Знать:** - основные термины по проблематике информационной безопасности	Пороговый уровень	Обучающийся слабо (частично) знает основные термины по проблематике информационной безопасности	**Блок А** **–**задания репродуктивного уровня – вопросы для обсуждения
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает основные термины по проблематике информационной безопасности	
			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает основные термины по проблематике информационной безопасности	

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*
		Уметь: **-** пользоваться современной научно-технической информацией по исследуемым проблемам и за	Пороговый уровень	Обучающийся слабо (частично) умеет пользоваться современной научно-технической информацией по исследуемым проблемам и за	**Блок В** – задания реконструктивного уровня – тематика рефератов и презентаций
			Базовый уровень	Обучающийся с незначительными затруднениями умеет пользоваться современной научно-технической информацией по исследуемым проблемам и за	
			Продвинутый уровень	Обучающийся умеет пользоваться современной научно-технической информацией по исследуемым проблемам и за	
		Владеть: - навыками поиска и использования нормативных и методических документов в целях решения задач профессиональной	Пороговый уровень	Обучающийся слабо (частично) владеет навыками поиска и использования нормативных и методических документов в целях решения	**Блок С** – задания практико-ориентированного уровня – практическая работа

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***
		деятельности		задач профессиональной деятельности	
			Базовый уровень	Обучающийся с небольшими затруднениями владеет навыками поиска и использования нормативных и методических документов в целях решения задач профессиональной деятельности	
			Продвинутый уровень	Обучающийся свободно владеет навыками поиска и использования нормативных и методических документов в целях решения задач профессиональной деятельности	

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

Для проверки сформированности компетенции ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
ИОПК-1.1. Использует основные понятия и определения в области информационных технологий и информационной безопасности

Блок А. Задания репродуктивного уровня («знать»)

А1. Тестовые задания

Выберите из предложенных один вариант

1. Основными характеристиками защищаемой информации являются:

a) конфиденциальность, целостность и статичность;

b) конфиденциальность, целостность и доступность;

c) аутентификация, целостность и доступность;

d)аутентификация, статичность и время создания;

2. Известность содержания информации только имеющим соответствующие полномочия субъектам – это:

a) Целостность;

b) Статичность;

c) Конфиденциальность;

d) Аутентификация;

3. Неизменность информации в условиях её случайного и (или) преднамеренного искажения и разрушения – это:

a) Целостность;

b) Конфиденциальность;

c) Доступность;

d) Идентификация;

4. Возможность получения информации или информационной услуги за приемлемое время – это:

a) конфиденциальность;

b) целостность;

c) доступность;

d) статичность;

5. Потенциально возможное событие, действие, процесс или явление, которое может привести к изменению функционирования компьютерной системы:

a) уязвимость;

b) атака;

c) угроза;

d) нет верного ответа;

6. Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого её состояния, при котором создаются условия для реализации угроз безопасности информации - это:

a) атака;

b) угроза;

c) уязвимость;

d) статичность;

7. Действия, предпринимаемые злоумышленником, которые заключаются в поиске и использовании уязвимостей информации – это:

a) статичность;

b) атака;

c) угроза;

d) изъян;

8. Классификацию угроз ИБ можно выполнить по нескольким критериям:

a) по аспекту информационной безопасности;

b) по компонентам информационной системы;

c) по способу осуществления;

d) все ответы верны;

9. Конфиденциальная информация может быть разделена на:

a) предметную и служебную;

b) служебную и закрытую;

c) предметную и открытую;

d) открытую и закрытую;

10. Целостность информации может быть разделена на:

a) статическую и динамическую;

b) статическую и служебную;

c) служебную и динамическую;

d) все верно;

11. Примером нарушения статической целостности не является:

a) ввод неверных данных;

b)несанкционированное изменение данных;

c)изменение программного модуля вирусом;

d) внесение дополнительных пакетов в сетевой трафик;

12. Примером нарушения динамической целостности не является:

a) нарушение атомарности транзакций;

b) внесение дополнительных пакетов в сетевой трафик;

c) несанкционированное изменение данных;

d) дублирование данных;

13. Угроза отказа служб может быть разбита на следующие типы:

a) отказ пользователей;

b) внутренний отказ информационной системы;

c) отказ поддерживающей инфраструктуры;

d) все ответы верны;

14. Что не относится к внутреннему отказу ИС:
a) ошибки при переконфигурировании системы;
b) отказы программного и аппаратного обеспечения;
c) разрушение данных;
d) нарушение работы систем связи;
15. Что не относится к отказу служб:
a) нарушение работы систем связи;
b) разрушение и повреждение помещений;
c) нарушение работы электропитания;
d) разрушение данных;
16. Нарушители" классифицируются по одному из следующих критериев:
a) уровень профессиональной подготовки противника;
b) тип доступа противника к системе;
c) способы атаки;
d) все ответы верны;
17. Высококвалифицированный специалист, стремящейся обойти защиту компьютерной системы:
a) Крякер;
b) Хаб;
c) Хакер;
d) Юзер;
18. Наибольшую угрозу ИС составляют:
a) Юзер;
b) Агент;
c) Хакер;
d) Крякер;
19. На сколько больших классов делятся каналы утечки информации:
a) Два;
b) Три;
c) Четыре;
d) Пять;
20.Что не относится к косвенным каналам утечки информации:
a) дистанционное видеонаблюдение;
b) использование полущивающих устройств;
c) перехват побочных электромагнитных излучений и наводок;
d) хищение носителей информации;

Блок В. Выберите верный вариант ответа:

21. Какая угроза отказа служб устраняется административно-правовыми методами:
a) отказ пользователей;
b) отказ программного обеспечения;
c) нарушение работ систем связи;

d) разрушение и повреждение помещений

22. К каналам, предполагающим изменение элементов информационной структуры относится:

a) намеренное копирование файлов и носителей информации;

b)маскировка под других пользователей, путём похищение идентифицирующей их информации;

c) хищение носителей информации;

d) незаконное подключение специальной регистрирующей аппаратуры к устройствам связи.

23. Что относится к каналам, не требующим изменение элементов ИС?

a)намеренное копирование файлов и носителей информации;

b)незаконное подключение специальной регистрирующей аппаратуры;

c)злоумышленное изменение программ;

d)злоумышленный вывод из строя средств защиты информации;

24. Какая направленность атак неверно сформулирована?

a) атаки на уровне операционной системы;

b) атаки на уровне системного администратора;

c) атаки на уровне сетевого программного обеспечения;

d) атаки на уровне систем управления базами данных.

25.К какому типу атак относится прослушивание передаваемых сообщений:

a) Пассивная атака;

b) Модификация потока данных;

c) Повторное использование;

d) Отказ в обслуживании.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тематика рефератов и презентаций

1. Информационная безопасность в условиях функционирования в России глобальных сетей.
2. Основные задачи информационной безопасности.
3. Основные методы обеспечения защиты информационной системы.
4. Современные поисковые системы. Методики поиска.
5. Уязвимости современных операционных систем.
6. Методика построения защищенного рабочего места с выходом в глобальную сеть.
7. Эмуляторы и создание образов дисков.
8. Методики защиты условно бесплатных программ.
9. Троянские программы.
10. "Черви", методика внедрения.

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

С1. Практические работы

Практическое занятие № 1 Политика «Требования по обеспечению информационной безопасности»

Цель: рассмотрение основных и наиболее важных моментов при разработке политики «Требования по обеспечению информационной безопасности» для выбранной КИС.

Задачи: формализовать требования по обеспечению безопасности ресурсов КИС в соответствии с действующим законодательством.

Ход работы

Преступим к разработке политики безопасности «Требования по обеспечению информационной безопасности (ИБ)» для выбранной КИС. Выделим следующие разделы для будущего документа:

1. Общие положения;
2. Рабочее место пользователя;
3. Парольная политика;
4. Работа с электронной почтой;
5. Работа в сети Интернет;
6. Действия в нестандартных ситуациях;
7. Ответственность.

Практическое занятие № 2 Политика «Обработка персональных данных в организации»

Цель занятия: рассмотрение основных и наиболее важных моментов при разработке политики «Обработка персональных данных в организации» для выбранной организации в соответствии с требованиями законодательства о ПДн .

Задачи: определить принципы, порядок и условия обработки персональных данных (ПДн) абонентов, работников организации и иных лиц, чьи ПДн обрабатываются организацией, а также третьими лицами по поручению организации.

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1. Контрольные вопросы

1. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
2. Место информационной безопасности экономических систем в национальной безопасности страны.

3. Концепция информационной безопасности.
4. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
5. Понятие информационного сервиса безопасности. Виды сервисов безопасности.
6. Идентификация и аутентификация. Основные методы идентификации и аутентификации.
7. Сервисы управления доступом.
8. Протоколирование и аудит.
9. Основы защиты корпоративных экономических информационных систем.
10. Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”).
11. Руководящие документы Гостехкомиссии России.
12. Международные стандарты информационной безопасности.

Для проверки сформированности компетенции ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

ИОПК-1.2. Классифицирует и оценивает угрозы информационной безопасности

Блок А. Задания репродуктивного уровня («знать»)

А1. Вопросы для обсуждения

1. Классификация источников угроз ИБ.
2. Классификация угроз ИБ.
3. Понятие атаки на информационные системы, классификация атак.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тематика рефератов и презентаций

1. Угрозы вычислительных сетей
2. Классификация угроз операционных систем
3. Угрозы, связанные с человеческим фактором

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

С1. Практические работы

Практическая работа «Построение концепции информационной безопасности предприятия»

Цель работы Знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры.

Краткие теоретические сведения

Концепция информационной безопасности используется для:

- принятия обоснованных управленческих решений по разработке мер защиты информации;
- выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
- координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;
- и, наконец, для формирования и реализации единой политики в области обеспечения информационной безопасности**.**

Задание

Разработать концепцию информационной безопасности компании (см. вариант выше), содержащую следующие основные пункты (приведен **примерный** план, в который в случае необходимости могут быть внесены изменения):

1. Общие положения

1.1. Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

- Классификации угроз.
- Основные непреднамеренные искусственные угрозы.
- Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы

3. Механизмы обеспечения информационной безопасности Предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия

4.1. Организационное обеспечение информационной безопасности.

- Задачи организационного обеспечения информационной безопасности.
- Подразделения, занятые в обеспечении информационной безопасности.
- Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

- Общие положения.
- Защита информационных ресурсов от несанкционированного доступа.
- Средства комплексной защиты от потенциальных угроз.
- Обеспечение качества в системе безопасности.
- Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

- Правовое обеспечение юридических отношений с работниками Предприятия .
- Правовое обеспечение юридических отношений с партнерами Предприятия.
- Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

5. Программа создания системы информационной безопасности Предприятия

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1. Контрольные вопросы

1. Классификация источников угроз ИБ.
2. Классификация угроз ИБ.
3. Понятие атаки на информационные системы, классификация атак.

Для проверки сформированности компетенции ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности

ИОПК-8.1. Анализирует научно-техническую литературу, нормативные и методические документы в целях решения задач профессиональной деятельности

Блок А. Задания репродуктивного уровня («знать»)

А1. Вопросы для обсуждения

4. Многообразие понятия «информационная безопасность» (ИБ), смежные понятия.
5. Место ИБ в системе национальной безопасности РФ.
6. Информационная война, информационный терроризм, киберпреступность и т.п., понятия и проблемы.
7. Региональные проблемы информационной безопасности.
8. Современное состояние проблем безопасности и защиты информации (технические аспекты).
9. Современное состояние проблем ИБ (гуманитарные аспекты), взаимосвязь с техническими аспектами.
10. Доктрина информационной безопасности РФ – структура, объект защиты.
11. Доктрина информационной безопасности РФ – основные источники угроз ИБ РФ.
12. Доктрина информационной безопасности РФ – основные угрозы ИБ РФ.
13. Доктрина информационной безопасности РФ – основные задачи по обеспечению ИБ РФ.
14. Законодательство в сфере ИБ, основные правовые акты и регламенты.
15. Понятие об идентификации и аутентификации субъектов и объектов доступа.
16. НСД к информации, его место в проблеме ИБ, модели разграничения доступа.
17. Этапы нарушения безопасности информационных систем, разнообразие и классификация средств.
18. Уязвимости ИС, атака – интерпретация в терминах метамодели ОСЗ.
19. Конфиденциальность, целостность, доступность информации. Определение и разнообразие нарушений.
20. Материальные среды и каналы утечки информации.

21. Разнообразие и классификация средств защиты информации.
22. Основные понятия и терминология нормативных документов по ИБ.
23. Назначение и содержание профиля защиты.
24. Назначение и содержание задания по безопасности.
25. Понятие об аудите и мониторинге безопасности ИС, методы и средства.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Тематика рефератов и презентаций

1. Настройки защиты электронной почты.
2. Технические методы защиты.
3. Косвенные каналы утечки информации и методики противодействия.
4. Защита от сетевых атак.
5. Модели доступа к данным.
6. Реализация дискреционной модели в операционных системах семейства Windows.
7. Основные нормативные руководящие документы, касающиеся государственной тайны.
8. Руководящие документы Гостехкомиссии России. ГОСТы в области информационной безопасности.
9. Доктрина информационной безопасности России и реальности ее осуществления.

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

С1. Практические работы

Практическая работа № 1 «Государственное регулирование информационной безопасности»

Цель работы: Поиск нормативных документов, регламентирующих информационную безопасность и защиту информации с помощью СПС «Консультант+»

1. Найти документы о защите информации; о защите персональных данных.
2. Найти документы о безопасности автоматизированных банковских систем; о безопасности оборудования информационных технологий.
3. Найти документы о информационной безопасности государства, объекта информатизации, понятии информационной безопасности.
4. Найти документы о криптографической защите информации.
5. Систематизировать названия найденных документов по типам (положение, кодекс, закон, указ, приказ и т.п.), расположив их на разных листах в

файле EXCEL. Вычислить количество каждого типа документов и отобразить его на новом листе.

6. В таблице EXCEL рядом с каждым названием документа в соседнем столбце ввести краткое резюме, основную мысль данного документа – не более 2…3 предложений.

Практическая работа №2 «Изучение законодательной базы в области конфиденциальной информации»

Цель работы: Познакомиться с правовыми документами направленными на поддержание законодательного уровня обеспечения информационной безопасности. Научиться аннотировать правовые документы.

Задание:

1) Используя справочно-правовую систему Консультант Плюс, заполните таблицу следующего вида, включив в нее не менее 15 видов тайн, касающихся экономической сферы деятельности

Таблица . Виды информационных тайн

Вид тайны	Краткое содержание -	Ссылка на правовой документ
Персональные данные	О фактах, событиях жизни гражданина, позволяющая идентифицировать личность	

Блок Д. Задания для использования в рамках промежуточной аттестации

Д1. Контрольные вопросы к зачету

13. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
14. Место информационной безопасности экономических систем в национальной безопасности страны.
15. Концепция информационной безопасности.
16. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
17. Понятие информационного сервиса безопасности. Виды сервисов безопасности.
18. Идентификация и аутентификация. Основные методы идентификации и аутентификации.
19. Сервисы управления доступом.
20. Протоколирование и аудит.
21. Основы защиты корпоративных экономических информационных систем.
22. Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”).

23. Руководящие документы Гостехкомиссии России.
24. Международные стандарты информационной безопасности.

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).

Для студентов очно-заочной формы обучения применятся 4-балльная и бинарная шкалы оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся.

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 и проектов	0-20	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Ответы на устные вопросы	0-10	«неудовлетворительно» «удовлетворительно»

		«хорошо» «отлично»
Тестирование	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение презентации	0-5	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Выполнение и публичная защита реферата	0-5	«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.
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	«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.
4-5	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.
0-3	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.

Тема реферата выбирается студентом самостоятельно из предложенного списка с учетом минимизации количества повторений выбранных тем. На написание реферата отводится одна неделя. Реферат оформляется согласно действующим в Дагестанском государственном университете народного хозяйства требованиям к оформлению письменных работ. Объем представленного реферата должен быть не менее 10 страниц машинописного текста без учета титульного листа.

Публичная защита реферата проводится в присутствии остальных студентов, защищающих рефераты. На выступление отводится не более 5 минут. Во время выступления студент должен обозначить основную цель реферата, а также цельно сформулировать базовую идею, отраженную в реферате.

Методика оценивания выполнения рефератов

Баллы	Оценка	Показатели	Критерии
5	Отлично	1. Полнота выполнения рефератов; 2. Своевременность выполнения; 3. Правильность ответов на вопросы.	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.
3-4	Хорошо		Основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.
1-2	Удовлетворительно		Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы.
0	Неудовлетворительно		Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы

Тема презентации выбирается студентом самостоятельно из предложенного списка с учетом минимизации количества повторений выбранных тем. На подготовку презентации отводится одна неделя.

Публичная презентация проводится в присутствии остальных студентов. На

выступление отводится не более 5 минут. Во время выступления студент должен обозначить основную цель презентации, а также цельно сформулировать базовую идею.

Методика оценивания выполнения презентаций

Баллы	**Оценка**	***Показатели***	***Критерии***
5	Отлично	1. Полнота выполнения презентаций; 2. Своевременность выполнения; 3. Правильность ответов на вопросы; 4. и т.д.	Выполнены все требования к составлению презентаций: дизайн слайдов, логика изложения материала, текст хорошо написан и сформированные идеи ясно изложены и структурированы
3-4	Хорошо		Основные требования к презентациям выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем презентации
1-2	Удовлетворительно		Имеются существенные отступления от требований к презентациям. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании презентаций или при ответе на дополнительные вопросы.
0	Неудовлетворительно		Тема презентации не раскрыта, обнаруживается существенное непонимание проблемы

Практические задания/проекты выполняются непосредственно во время занятий семинарского типа (одно задание на одну пару согласно текущей тематике занятия). Студенты должны выполнять задание самостоятельно, но имеют возможность обратиться к преподавателю за разъяснениями постановки задачи или оценкой правильности представленного решения. Если преподаватель вынужден разъяснять аспекты непосредственного выполнения задания, то это негативно отражается на оценке выполняющего задание студента..

Методика оценивания выполнения практических работ/проектов

Баллы	***Оценка***	***Показатели***	***Критерии***

18-20	«отлично»	1. Полнота выполнения проекта; 2. Своевременность выполнения; 3. Правильность ответов на вопросы; 4. и т.д.	Основные требования к выполнения проекта выполнены. Продемонстрировано умение анализировать ситуацию и находить оптимальное количества решений, умение работать с информацией, в том числе умение затребовать дополнительную информацию, необходимую для достижения поставленной цели
14-17	«хорошо»		Основные требования к выполнению проекта реализованы, но при этом допущены недочеты. В частности, недостаточно раскрыты навыки критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки, креативности, нестандартности предлагаемых решений
11-13	«удовлетворительно»		Имеются существенные отступления от выполнения проекта. В частности отсутствуют навыки умения моделировать решения в соответствии с заданием, представлять различные подходы к разработке планов действий, ориентированных на конечный результат
0-10	«неудовлетвори-тельно»		Задача выполнения проекта не раскрыта, обнаруживается существенное непонимание проблемы

Лист актуализации оценочных материалов по дисциплине «Основы информационной безопасностью»

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 _____