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 «МОНИТОРИНГ И АУДИТ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В АВТОМТИЗИРВАННЫХ СИСТЕМАХ»

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

Уровень высшего образования - бакалавриат

.

Махачкала – 2023

УДК 681.518(075.8)
ББК 32.81.73

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

Внутренний рецензент – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, заведующий кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

Внешний рецензент – Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры "Математические методы в экономике" Дагестанского государственного университета.

Представитель работодателя - Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза».

Оценочные материалы по дисциплине «Мониторинг и аудит защищенности информации в автоматизированных системах» 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 «Мониторинг и аудит защищенности информации в автоматизированных системах» размещены на официальном сайте www.dgunh.ru

Эмирбеков Э.М. Оценочные материалы по дисциплине «Мониторинг и аудит защищенности информации в автоматизированных системах» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2023 г. – 26 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 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», 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 «Мониторинг и аудит защищенности информации в автоматизированных системах» на соответствие их учебных достижений поэтапным требованиям образовательной программы высшего образования 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем»

Оценочные материалы по дисциплине «Мониторинг и аудит защищенности информации в автоматизированных системах» 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-3	Способен учитывать и использовать особенности средств защиты информации при формировании системы защиты информации автоматизированных систем

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-3. Способен учитывать и использовать особенности средств защиты информации при формировании системы защиты информации автоматизированных систем	ИПК-3.1 Проводит анализ уязвимости программных и программно-аппаратных средств системы защиты информации и экспертизу состояния защищенности информации автоматизир	**Знать:** – способы проведения проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	Пороговый уровень	Обучающийся слабо (частично) знает способы проведения проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	**Блок А –**задания репродуктивного уровня – вопросы для обсуждения
			Базовый уровень	Обучающийся с незначительными ошибками и отдельными пробелами знает способы проведения проверки работоспособности и эффективности применяемых	

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*
	ованных систем с использованием современного инструментария и интеллектуальных информационно-аналитических систем			программно-аппаратных средств защиты информации	
			Продвинутый уровень	Обучающийся с требуемой степенью полноты и точности знает способы проведения проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	
		<u>Уметь:</u> – проводить анализ уязвимости программных и программно-аппаратных средств системы защиты информации и экспертизу состояния защищенности информации автоматизированных	Пороговый уровень	Обучающийся слабо (частично) умеет проводить анализ уязвимости программных и программно-аппаратных средств системы защиты информации и экспертизу состояния защищенности информации автоматизированных систем	**Блок В** – задания реконструктивного уровня — контрольная работа - Тестовые задания ё
			Базовый уровень	Обучающийся с незначительными затруднениями умеет проводить анализ уязвимости программных 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*
		систем		программно-аппаратных средств системы защиты информации и экспертизу состояния защищенности информации автоматизированных систем	
			Продвинутый уровень	Обучающийся умеет проводить анализ уязвимости программных и программно-аппаратных средств системы защиты информации и экспертизу состояния защищенности информации автоматизированных систем	
		Владеть: – навыками проведения контрольных проверок работоспособности и эффективности применяемых программны	Пороговый уровень	Обучающийся слабо (частично) владеет навыками проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	**Блок С** – задания практико-ориентированного уровня - лабораторная 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*
		х, программно-аппаратных средств защиты	Базовый уровень	Обучающийся с небольшими затруднениями владеет навыками проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	
			Продвинутый уровень	Обучающийся свободно владеет навыками проведения контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты	

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

Для проверки сформированности компетенции ПК-3. Способен учитывать и использовать особенности средств защиты информации при формировании системы защиты информации автоматизированных систем
ИПК-3.1. Проводит анализ уязвимости программных и программно-аппаратных средств системы защиты информации и экспертизу состояния защищенности информации автоматизированных систем с использованием современного инструментария и интеллектуальных информационно-аналитических систем

Блок А. Задания репродуктивного уровня («знать»)

А1. Вопросы для обсуждения

1. Цели и задачи, решаемые СУИБ.
2. Стандартизация в области построения СУИБ: сходства и различия стандартов.
3. Стратегии выбора области деятельности СУИБ.
4. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
5. Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
6. Политика ИБ и политика СУИБ: сходства и различия.
8. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса рамках СУИБ.
10. Анализ рисков ИБ: основные подходы, основные этапы процесса.
11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
16. Внедрение процессов управления ИБ: этапы и последовательность.
17. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения.
18. Аудит ИБ.

19. Сертификация в сфере ИБ.
20. Анализ рисков ИБ.
21. Оценка рисков ИБ.
22. Моделирование угроз ИБ.
23. Программные средства аудита ИБ.
24. Инциденты ИБ.
25. DLP.
26. Облачная безопасность.
27. Тесты на проникновение.
28. Безопасность АСУ ТП.
29. Внутренние и внешние аудиты ИБ: цели и задачи процессов, сходства и различия.
30. Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ, обеспечение соответствия требованиям законодательства.
31. Документационное обеспечение СУИБ: понятия документа и записи, иерархия документов системы управления ИБ.
32. Мониторинг эффективности мер по обеспечению ИБ и процессов управления ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
33. Процессы улучшения системы управления ИБ: основные процессы, из взаимосвязь и роль в рамках СУИБ.
34. Корректирующие/предупреждающие действия: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.

Блок В. Задания реконструктивного уровня («уметь»)

В1. Контрольные вопросы

1. Назовите критерии, согласно которым происходит выбор решения программно-аппаратных и технических средств защиты информации.
2. Обоснуйте необходимость участия пользователя в создании проектной документации в процессе создания ИС и ИТ.
3. Охарактеризуйте наиболее часто применяемые методы и варианты организации создания информационных систем и информационных технологий в управлении.
4. Охарактеризуйте понятие и определите назначение онтологии предметной области
5. Угрозы ИБ и их источники
6. Модель построения системы информационной безопасности предприятия
7. Разработка концепция обеспечения ИБ
8. Понятие аудита безопасности
9. Методы анализа данных при аудите ИБ

10. Анализ информационных рисков предприятия. Методы оценивания информационных рисков
11. Задачи и содержание работ при проведении аудита ИБ
12. Подготовка предприятий к проведению аудита ИБ
13. Планирование процедуры аудита ИБ
14. Организация и проведения работ по аудиту
15. Алгоритм проведения аудита безопасности предприятия
16. Перечень и систематизация данных, необходимых для проведения аудита ИБ
17. Выработка рекомендаций и подготовка отчетных документов
18. Экономическая оценка обеспечения ИБ

В2. Тестовые задания

1)Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

А). Поддержка высшего руководства
Б) Эффективные защитные меры и методы их внедрения
В). Актуальные и адекватные политики и процедуры безопасности
Г). Проведение тренингов по безопасности для всех сотрудников

2) Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

А) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
Б) Когда риски не могут быть приняты во внимание по политическим соображениям
В) Когда необходимые защитные меры слишком сложны
Г)Когда стоимость контрмер превышает ценность актива и потенциальные потери

3)Что такое политики безопасности?

А)Пошаговые инструкции по выполнению задач безопасности
Б)Общие руководящие требования по достижению определенного уровня безопасности
В)Широкие, высокоуровневые заявления руководства
Г) Детализированные документы по обработке инцидентов безопасности

4)Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

А)Анализ рисков
Б)Анализ затрат / выгоды
В) Результаты ALE
Г) Выявление уязвимостей и угроз, являющихся причиной риска

5) Что лучше всего описывает цель расчета ALE?

А)Количественно оценить уровень безопасности среды
Б) Оценить возможные потери для каждой контрмеры
В)Количественно оценить затраты / выгоды
Г)Оценить потенциальные потери от угрозы в год

6) Тактическое планирование – это:

А) Среднесрочное планирование
Б) Долгосрочное планирование
В). Ежедневное планирование
Г) Планирование на 6 месяцев

7)Что является определением воздействия (exposure) на безопасность?

А) Нечто, приводящее к ущербу от угрозы
Б) Любая потенциальная опасность для информации или систем
В) Любой недостаток или отсутствие информационной безопасности
Г) Потенциальные потери от угрозы

8) Эффективная программа безопасности требует сбалансированного применения:

А) Технических и нетехнических методов
Б) Контрмер и защитных механизмов
В) Физической безопасности и технических средств защиты
Г) Процедур безопасности и шифрования

9) Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

А) Внедрение управления механизмами безопасности
Б) Классификацию данных после внедрения механизмов безопасности
В) Уровень доверия, обеспечиваемый механизмом безопасности
Г). Соотношение затрат / выгод

10) Как рассчитать остаточный риск?

А) Угрозы х Риски х Ценность актива

Б) (Угрозы х Ценность актива х Уязвимости) х Риски
В) SLE х Частоту = ALE
Г)(Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

11)Что из перечисленного не является целью проведения анализа рисков?

А) Делегирование полномочий
Б) Количественная оценка воздействия потенциальных угроз
В) Выявление рисков
Г) Определение баланса между воздействием риска и стоимостью необходимых контрмер

12) Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?
А) Поддержка
Б) Выполнение анализа рисков
В) Определение цели и границ
Г)Делегирование полномочий

13) Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

А) Чтобы убедиться, что проводится справедливая оценка
Б) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
В) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
Г) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

14)Что является наилучшим описанием количественного анализа рисков?

А) Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
Б) Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
В) Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
Г) Метод, основанный на суждениях и интуиции

15) Почему количественный анализ рисков в чистом виде не достижим?

А) Он достижим и используется
Б) Он присваивает уровни критичности. Их сложно перевести в денежный вид.
В) Это связано с точностью количественных элементов
Г) Количественные измерения должны применяться к качественным элементам

16) Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

А) . Много информации нужно собрать и ввести в программу
Б) Руководство должно одобрить создание группы
В) Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
Г) Множество людей должно одобрить данные

17) Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

А) Список стандартов, процедур и политик для разработки программы безопасности
Б) Текущая версия ISO 17799
В) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
Г) Открытый стандарт, определяющий цели контроля

18) Из каких четырех доменов состоит CobiT?

А) Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
Б) Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
В) Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
Г) Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

19) Что представляет собой стандарт ISO/IEC 27799?

А) Стандарт по защите персональных данных о здоровье
Б) Новая версия BS 17799
В) Определения для новой серии ISO 27000
Г) Новая версия NIST 800-60

20) Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

А) Анализ связующего дерева
Б) AS/NZS
В)NIST
Г) Анализ сбоев и дефектов

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

С1. Лабораторные работы

Лабораторная работа №1 «Сравнительный анализ методик проведения аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ)»

Основные принципы аудита информационной безопасности

-Понятие «аудит информационной безопасности объекта»

-Этапы проведения аудита информационной безопасность

Лабораторная работа №2 «Систематизация угроз информации, информационным ресурсам и услугам, информационной безопасности»

Лабораторная работа №3 «Тестирование автоматизированных решений аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ)»

Лабораторная работа №4. «Методология проведения аудита информационной безопасности объекта»;

-Основные принципы аудита информационной безопасности

-Понятие «аудит информационной безопасности объекта»

-Этапы проведения аудита информационной безопасность

Лабораторная работа №5. «Сбор исходных данных для аудита информационной безопасности АИС»;

-Критерии аудита информационной безопасности

-Что является исходными данными для аудита информационной безопасности АИС

-Как происходит сбор исходных данных для аудита информационной безопасности?

Лабораторная работа №6. «Выявление уязвимостей информационной системы»;

-Понятие «уязвимость» -Виды уязвимостей информационной системы

-Методика анализа защищенности ИС

-Как происходит выявление уязвимостей информационной системы?

Лабораторная работа №7. «Определение рисков от реализации угроз АИС;
-Понятие «риск»
-Методы оценки рисков информационной безопасности
-Какие существуют этапы проведения анализа рисков?

Лабораторная работа №8. Идентификация защитных механизмов для АИС»;
-Что такое идентификация.
-Что такое защитный механизм.
-Приведите примеры защитных механизмов.
-Назовите основные защитные механизмы, используемые в системах защиты информации.
-Как происходит идентификация защитных механизмов.

Лабораторная работа №9. «Идентификация нарушителей в АИС».
-Что такое идентификация.
-Кто такие нарушители.
-Приведите примеры нарушителей.
-Как можно идентифицировать нарушителей?
-Перечислите виды нарушителей.
Лабораторная работа №10. «Аудит информационных процессов в операционных системах Windows»
Цель знакомство с организацией аудита информационных процессов в сетевых операционных системах Windows
Порядок выполнения работы:
1. Познакомьтесь с программой просмотра событий. Познакомьтесь с различными видами журналов, их структурой. Приведите отрывки журналов в отчете, дайте интерпретацию отдельных записей журналов.
2. Познакомьтесь с возможностями настройки журналов, параметрами фильтрации записей.
Сохраните журнал в текстовом виде и экспортируйте его в Excel.
3. Ознакомьтесь с аудитом доступа к объектам. Установите определенные права аудита на созданный Вами каталог и вложенные в него файлы. Приведите их в вашем отчете. Произведите операции с этими файлами, приведите их в отчете и проанализируйте события появляющиеся в журнале безопасности.
4. Включите аудит входов в систему и событий входа в систему, исследуйте события, отнесенные к данной категории аудита, дайте интерпретацию информации, выдаваемой для отдельных событий.
Проведите анализ связи отдельных событий, сделайте выводы по результатам анализа.
5. Исследуйте аудит управления учетными записями.
6. Исследуйте аудит использования привилегий.
7. Исследуйте аудит изменения политик.
8. Познакомьтесь с аудитом системных событий
9. Исследуйте возможности аудита процессов.

Требования к отчету

Отчет должен оформляться в электронном и печатном виде на листах формата А4 и содержать задание, краткие необходимые теоретические сведения, полученные по каждому пункту задания результаты и выводы.

Результаты исследования отдельных категорий аудита должны включать описание, как проводились исследования, примеры различных событий данной категории, интерпретацию информации, выдаваемой для отдельных событий, анализ связи отдельных событий, полученные результаты и сделанные результаты и выводы.

Д1.Перечень экзаменационных вопросов

1. Общие положения по аудиту ИБ автоматизированных информационных систем (АИС). Существующие проблемы аудита ИБ АИС.
2. Понятие системы мониторинга информационной безопасности.
3. Типовое содержание и последовательность проведения аудита ИБ АИС.
4. Компоненты программно-технической часть системы мониторинга информационной безопасности.
5. Порядок проведения аттестационных испытаний объектов вычислительной техники и автоматизированных систем в ходе аудита ИБ.
6. Документационная часть системы мониторинга информационной безопасности.
7. Состав и характеристика отчетных документов по результатам аудита ИБ автоматизированных информационных систем.
8. Кадровая составляющая системы мониторинга информационной безопасности.
9. . Характеристика этапа сбора предварительной информации для анализа защищенности всего информационного ресурса и выявление проблемных вопросов в области ИБ предприятия.
10. Основные этапы создания системы мониторинга информационной безопасности.
11. Порядок проведения аудита комплексной безопасности информационных объектов на предприятии.
12. Виды мониторинга информационной безопасности
13. Основные меры аудита комплексной безопасности.
14. Функции мониторинга безопасности информационной системы.
15. Порядок анализа инцидентов.
16. Мониторинг работоспособности аппаратных компонент автоматизированных систем.

17. Нормативно-правовые основы по организации и проведению аудита ИБ.
18. Метод мониторинга безопасности при функционировании инфокоммуникационных систем.
19. Основные направления деятельности в области аудита ИБ.
20. Структура системы мониторинга.

Блок Д. Задания для использования в рамках промежуточной аттестации

Д2.Перечень задач к экзамену:

1. Разработайте новое правило анализа событий мониторинга для заданных событий.
2. Привести примеры реализации элементов модели измерения и оценивания ИБ: атрибута, метода измерения, основной меры, функции измерения, производной меры, аналитической модели, показателя
3. Привести примеры свидетельств оценки ИБ, полученных в результате: проверки и анализа документов, относящихся к объекту оценки; наблюдения за процессами объекта оценки; опроса сотрудников объекта оценки
4. Сформировать анкеты для области оценки ИБ и универсальную шкалу измерения атрибутов
5. Проанализировать свидетельства аудита ИБ
6. Определить содержание отчёта и заключения по результатам аудита ИБ
7. Построить фрагмент методики оценки соответствия ИБ требованиям нормативных документов с использованием анкет для измерения атрибутов объекта оценки (для выбранной области обеспечения ИБ)
8. Представить общую форму метрики для измерения или оценивания атрибута
9. Построить фрагмент методики оценки соответствия ИБ требованиям нормативных документов с использованием метрик для измерения атрибутов объекта оценки (для выбранной области обеспечения ИБ)
10. Сформировать программу аудита ИБ для выбранных областей обеспечения ИБ объекта

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 лабораторных заданий	0-20	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Контрольная работа	0-30	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Ответы на устные вопросы	0-10	«неудовлетворительно» «удовлетворительно» «хорошо» «отлично»
Тестирование	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
8-10	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
6-7	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.
3-5	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.
0-2	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 оценивание ответов на устные вопросы

Баллы	Оценка	Показатели	Критерии
9-10	Отлично	1. Полнота данных ответов; 2. Аргументированность данных ответов; 3. Правильность ответов на вопросы;	Полно и аргументировано даны ответы по содержанию задания. Обнаружено понимание материала, может обосновать свои суждения, применить знания на практике, привести

		4. и т.д.	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.
4-6	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.
0-3	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.

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 лабораторных работ

Баллы	Оценка	Показатели	Критерии
18-20	Отлично	1. Полнота выполнения заданий 2. Выполнение дополнительных заданий 3. Подготовка отчета	- правильно выполнены все задания лабораторной работы в соответствии с требованиями; - правильно выполнены дополнительные задания; - своевременно предоставлен отчет о выполнении работы.
15-18	Хорошо		- правильно выполнены все задания в основной части; - дополнительные задания выполнены не в полном объеме; - предоставлен отчет о выполнении работы, либо в случае несвоевременного предоставления отчета или с наличием несущественных ошибок в выполнении лабораторных заданиях
11-15	Удовлетворительно		- выполнены не все, но более 50% заданий лабораторной работы; - дополнительные задания не выполнены, - несвоевременно предоставлен отчет о выполнении работы.
0-10	Неудовлетворительно		- выполнено менее 50% лабораторной работы; - не выполнены дополнительные задания; - отчет о выполнении работы не предоставлен

Контрольная работа проводится раз в семестр.

Методика оценивания ответов письменные работы

Баллы	Оценка	Показатели	Критерии
25-30	«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.
19-24	«хорошо»		Студент дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет.
15-18	«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.
0-14	«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.

Итоговыми формами контроля по дисциплине является экзамен. Экзамен проводится в виде письменного ответа на заданный вопрос. Каждому студенту предлагается 2 вопроса, каждый из которых оценивается максимум на 15 баллов. При оценке ответа на вопрос оценивается полнота ответа, точность формулировок, правильное цитирование соответствующих законодательных актов, наличие иллюстративных примеров.

Лист актуализации оценочных материалов по дисциплине «Мониторинг и аудит защищенности информации в автоматизированных системах»

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 _____