Приложение А
(обязательное к рабочей программе дисциплины)

Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Технология построения защищенных автоматизированных систем»

Уровень образования **бакалавриат**
(бакалавриат/магистратура/специалитет)

Направление **10.03.01 Информационная безопасность**
(код, наименование специальности)

Профиль **Безопасность автоматизированных систем**
(наименование)

Разработчик _____ Качаева Г.И.
подпись (ФИО уч. степень, уч. звание)

Фонд оценочных средств обсужден на заседании кафедры ИБ «20» сентября 2021г., протокол №_2

Зав. кафедрой _____ Качаева Г.И.
подпись (ФИО уч. степень, уч. звание)

г. Махачкала 2021

СОДЕРЖАНИЕ

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины «Технология построения защищенных автоматизированных систем» и предназначен для контроля и оценки образовательных достижений обучающихся (в т.ч. по самостоятельной работе студентов, далее – СРС), освоивших программу данной дисциплины.

Целью фонда оценочных средств является установление соответствия уровня подготовки обучающихся требованиям ФГОС ВО по направлению 10.03.01 Информационная безопасность.

Рабочей программой дисциплины «Технология построения защищенных автоматизированных систем» предусмотрено формирование следующей компетенции:

УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ОПК-4Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности

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

ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов.

ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений

2. Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля)

Описание показателей и критериев оценивания компетенций, формируемых в процессе освоения дисциплины (модуля), и используемые оценочные средства приведены в таблице 1.

Перечень оценочных средств, рекомендуемых для заполнения таблицы 1 (в ФОС не приводится, используется только для заполнения таблицы)

- *Устный опрос*
- *Тесты*
- *Вопросы для проведения экзамена*

2.1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОПОП

Таблица 1

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	Критерии оценивания	Наименование контролируемых разделов и тем[1]
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.2.1 умеет разрабатывать и реализовывать этапы проекта в сфере профессиональной деятельности	- знает и умеет разрабатывать и реализовывать этапы проекта в сфере профессиональной деятельности **на удовлетворительно** - знает и умеет разрабатывать и реализовывать этапы проекта в сфере профессиональной деятельности **на хорошо** - знает и умеет разрабатывать и реализовывать этапы проекта в сфере профессиональной деятельности **на отлично**	Тема 1: Основные определения и свойства открытых систем Тема 2: Модели среды открытых информационных систем
ОПК-4Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1.13 знает современные виды информационного взаимодействия и обслуживания телекоммуникационных сетей и систем ОПК-4.3.3 умеет определять характеристики сетей и систем телекоммуникаций, показатели качества предоставляемых услуг	- знает современные виды информационного взаимодействия и обслуживания телекоммуникационных сетей и систем на **удовлетворительно.** - знает современные виды информационного взаимодействия и обслуживания телекоммуникационных сетей и систем на **хорошо.** - знает современные виды информационного взаимодействия и обслуживания телекоммуникационных сетей и систем на **отлично.**	Тема 3: Профили открытых информационных систем
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в	ОПК-8.2.1 умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности ОПК-8.2.2 умеет различать факты, интерпретации, оценки и аргументи-	- знает и умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности на **удовлетворительно.** - знает и умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности на **хорошо.**	Тема 4: Методология построения профилей информационных систем

[1] *Наименования разделов и тем должен соответствовать рабочей программе дисциплины.*

целях решения задач профессиональной деятельности	рованно отстаивать свою позицию в процессе коммуникации	- знает и умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности на **отлично.**	
ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов.	ОПК-11.1.1знает типовые методы проведения измерений параметров, характеризующих наличие технических каналов утечки информации.	- знает типовые методы проведения измерений параметров, характеризующих наличие технических каналов утечки информации **на удовлетворительно** - знает типовые методы проведения измерений параметров, характеризующих наличие технических каналов утечки информации **на хорошо** - знает типовые методы проведения измерений параметров, характеризующих наличие технических каналов утечки информации **на отлично**	Тема 5: Объекты стандартизации в функциональных профилях информационных систем и источники базовых стандартов информационных технологий
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1.1 знает жизненные циклы управляемых процессов: жизненный цикл изделия, жизненный цикл программного продукта, реализуемого в информационной системе ОПК-12.1.3 знает методы, показатели и критерии технико-экономического обоснования проектных решений при разработке систем и средств обеспечения защиты информации с учетом действующих нормативных и методических документов.	- знает жизненные циклы управляемых процессов: жизненный цикл изделия, жизненный цикл программного продукта, реализуемого в информационной системе на **удовлетворительно.** - знает жизненные циклы управляемых процессов: жизненный цикл изделия, жизненный цикл программного продукта, реализуемого в информационной системе на **хорошо.** - знает жизненные циклы управляемых процессов: жизненный цикл изделия, жизненный цикл программного продукта, реализуемого в информационной системе на **отлично.**	Тема 6: Компонентная разработка приложений

2.1.2. Этапы формирования компетенций

Сформированность компетенций по дисциплине «Открытые информационные системы» определяется на следующих этапах:
1. **Этап текущих аттестаций** *(Для проведения текущих аттестаций могут быть использованы оценочные средства, указанные в разделе 2)*
2. **Этап промежуточных аттестаций** (*Для проведения промежуточной аттестации могут быть использованы другие оценочные средства*)

Таблица 2

Код и наименование формируемой компетенции	Код и наименование индикатора достижения формируемой компетенции	**Этапы формирования компетенции**					
		Этап текущих аттестаций					**Этап промежуточной аттестации**
		1-5 неделя	**6-10 неделя**	**11-15 неделя**	**1-17 неделя**		**18-20 неделя**
		Текущая аттестация №1	Текущая аттестация №2	Текущая аттестация №3	СРС	КР/КП	Промежуточная аттестация
1		**2**	**3**	**4**	**5**	**6**	**7**
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.2.1 умеет разрабатывать и реализовывать этапы проекта в сфере профессиональной деятельности	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
ОПК-4Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1.13 знает современные виды информационного взаимодействия и обслуживания телекоммуникационных сетей и систем ОПК-4.3.3 умеет определять характеристики сетей и систем телекоммуникаций, показатели качества предоставляемых услуг	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена

ОПК-8.Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.2.1 умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности ОПК-8.2.2 умеет различать факты, интерпретации, оценки и аргументированно отстаивать свою позицию в процессе коммуникации	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
ОПК-11.Способен проводить эксперименты по заданной методике и обработку их результатов.	ОПК-11.1.1знает типовые методы проведения измерений параметров, характеризующих наличие технических каналов утечки информации.	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена
ОПК-12.Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1.1 знает жизненные циклы управляемых процессов: жизненный цикл изделия, жизненный цикл программного продукта, реализуемого в информационной системе ОПК-12.1.3 знает методы, показатели и критерии технико-экономического обоснования проектных решений при разработке систем и средств обеспечения защиты информации с учетом действующих нормативных и методических документов.	Контрольная работа №1	Контрольная работа №2	Контрольная работа №3			Вопросы для проведения экзамена

СРС – самостоятельная работа студентов;
КР – курсовая работа;
КП – курсовой проект.

2.2. Показатели уровней сформированности компетенций на этапах их формирования, описание шкал оценивания

2.2.1. Показатели уровней сформированности компетенций на этапах их формирования

Результатом освоения дисциплины «Открытые информационные» системы является установление одного из уровней сформированности компетенций: высокий, повышенный, базовый, низкий.

Таблица 3

Уровень	Универсальные компетенции	Общепрофессиональные/ профессиональные компетенции
Высокий (оценка «отлично», «зачтено»)	Сформированы четкие системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные и верные. Даны развернутые ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции	Обучающимся усвоена взаимосвязь основных понятий дисциплины, в том числе для решения профессиональных задач. Ответы на вопросы оценочных средств самостоятельны, исчерпывающие, содержание вопроса/задания оценочного средства раскрыто полно, профессионально, грамотно. Даны ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции
Повышенный (оценка «хорошо», «зачтено»)	Знания и представления по дисциплине сформированы на повышенном уровне. В ответах на вопросы/задания оценочных средств изложено понимание вопроса, дано достаточно подробное описание ответа, приведены и раскрыты в тезисной форме основные понятия. Ответ отражает полное знание материала, а также наличие, с незначительными пробелами, умений и навыков по изучаемой дисциплине. Допустимы единичны е негрубые ошибки. Обучающимся продемонстрирован повышенный уровень освоения компетенции	Сформированы в целом системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные, грамотные. Продемонстрирован повышенный уровень владения практическими умениями и навыками. Допустимы единичные негрубые ошибки по ходу ответа, в применении умений и навыков
Базовый (оценка «удовлетворительно», «зачтено»)	Ответ отражает теоретические знания основного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП. Обучающийся допускает неточности в ответе, но обладает необходимыми знаниями для их устранения. Обучающимся продемонстрирован базовый уровень освоения компетенции	Обучающийся владеет знаниями основного материал на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продемонстрирован базовый уровень владения практическими умениями и навыками, соответствующий минимально необходимому уровню для решения профессиональных задач
Низкий (оценка «неудовлетворительно» «не зачтено»)	Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие практических умений и навыков	

Показатели уровней сформированности компетенций могут быть изменены, дополнены и адаптированы к конкретной рабочей программе дисциплины.

2.2.2. Описание шкал оценивания

В ФГБОУ ВО «ДГТУ» внедрена модульно-рейтинговая система оценки учебной деятельности студентов. В соответствии с этой системой применяются пятибальная, двадцатибальная и стобальная шкалы знаний, умений, навыков.

Шкалы оценивания			Критерии оценивания
пятибальная	двадцатибальная	стобальная	
«Отлично» - 5 баллов	«Отлично» - 18-20 баллов	«Отлично» - 85 – 100 баллов	Показывает высокий уровень сформированности компетенций, т.е.: – продемонстрирует глубокое и прочное усвоение материала; – исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; – правильно формирует определения; – демонстрирует умения самостоятельной работы с нормативно-правовой литературой; – умеет делать выводы по излагаемому материалу.
«Хорошо» - 4 баллов	«Хорошо» - 15 - 17 баллов	«Хорошо» - 70 - 84 баллов	Показывает достаточный уровень сформированности компетенций, т.е.: – демонстрирует достаточно полное знание материала, основных теоретических положений; – достаточно последовательно, грамотно логически стройно излагает материал; – демонстрирует умения ориентироваться в нормальной литературе; – умеет делать достаточно обоснованные выводы по излагаемому материалу.
«Удовлетворительно» - 3 баллов	«Удовлетворительно» - 12 - 14 баллов	«Удовлетворительно» - 56 – 69 баллов	Показывает пороговый уровень сформированности компетенций, т.е.: – демонстрирует общее знание изучаемого материала; – испытывает серьезные затруднения при ответах на дополнительные вопросы; – знает основную рекомендуемую литературу; – умеет строить ответ в соответствии со структурой излагаемого материала.
«Неудовлетворительно» - 2 баллов	«Неудовлетворительно» - 1-11 баллов	«Неудовлетворительно» - 1-55 баллов	Ставится в случае: – незнания значительной части программного материала; – не владения понятийным аппаратом дисциплины; – допущения существенных ошибок при изложении учебного материала; – неумение строить ответ в соответствии со структурой излагаемого вопроса; – неумение делать выводы по излагаемому материалу.

3. Типовые контрольные задания, иные материалы и методические рекомендации, необходимые для оценки сформированности компетенций в процессе освоения ОПОП

3.1. Задания и вопросы для входного контроля

1. Основные положения теории защиты информации.
2. Математическое моделирование в проектировании защищённых телекоммуникационных систем.
3. Классификация угроз безопасности информации в телекоммуникационных системах и их элементах.
4. Дискреционное разграничение доступа для обеспечения безопасности телекоммуникационных систем.
5. Мандатное разграничение доступа для обеспечения безопасности телекоммуникационных систем.
6. Ролевое разграничение доступа для обеспечения безопасности телекоммуникационных систем.
7. Изолированная программная среда в проектировании защищённых телекоммуникационных систем и их элементов..

3.2. Оценочные средства и критерии сформированности компетенций

Комплект заданий для контрольной работы №1 для первой аттестации

1. Классификация автоматизированных систем (АС)
2. Информационные технологии, используемые в АС
3. Жизненный цикл АС
4. Основные угрозы безопасности информации в автоматизированных системах
5. Отказоустойчивость АС
6. Основные понятия и классификация защищенных автоматизированных систем
7. Понятия информации и информационных ресурсов. Предмет защиты информации
8. Понятие информационной безопасности
9. Понятие политики информационной безопасности
10. Понятие системы защиты информации. Основные положения безопасности автоматизированных систем
11. Трехэтапная разработка мер по обеспечению безопасности автоматизированных систем
12. Стадия выработки требований
13. Стадия определения способов защиты
14. Стадия определения функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты
15. Основные принципы обеспечения информационной безопасности в автоматизированной системе

Комплект заданий для контрольной работы №2 для второй аттестации

1. Принципы, позволяющие реализовать положения по защите АС
2. Угрозы безопасности информации в защищенных автоматизированных системах
3. Базовые признаки угроз информационной безопасности. Классификация угроз
4. Уровни доступа к защищаемой информации
5. Подходы к обеспечению защиты информации. Сервисы безопасности
6. Виды аутентификации. Проблема надежной аутентификации и пути ее решения

7. Средства и методы хранения эталонных копий аутентификационной информации
8. Средства и методы защиты от компрометации и подбора паролей
9. Требования к защите компьютерной информации
10. Нормативные документы ФСТЭК, регламентирующие защиту информации от несанкционированного доступа
11. Основные подсистемы и группы механизмов защиты АС
12. Последовательность и содержание этапов разработки АС
13. Методы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем
14. Методы и средства обеспечения отказоустойчивости автоматизированных систем.
15. Критерии оценки защищенности АС
16. Методы обеспечения информационной безопасности АС. Организация коллективной разработки программного обеспечения АС

Комплект заданий для контрольной работы №3 для третьей аттестации

1. Проектирование защищенных АС. Основные методы проектирования
2. Основы ведения конструкторской документации
3. Структура и содержание технического задания
4. Построение комплексной защиты АС. Основы проектирования комплексной защиты информационной безопасности от НСД
5. Аттестация АС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации
6. Особенности эксплуатации АС на объекте защиты
7. Организация технического обслуживания защищенных АС
8. Аппаратно-программные средства диагностики АС
9. Протоколы аутентификации на прикладном уровне
10. Протоколы аутентификации на транспортном уровне
11. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI
12. Задачи администрирования подсистем АС. Средства администрирования АС
13. Настройка сетевой подсистемы защищенной АС
14. Принципы функционирования информационных сервисов АС
15. Установка и настройка работы информационных сервисов АС
16. Удаленное администрирование компонентов АС

Комплект заданий для проведения тестирования

Темы 1, 2, 3, 4, 5, 6

Выберите правильные ответы.

1. Автоматизированная система - это:

- А) Система, состоящая из АРМ, серверов и СКС
- В) Компьютерная сеть
- С) Система, состоящая из персонала, пользователей и комплекса средств автоматизации.

2. Информационная система - это:

- А) Система, состоящая из персонала, пользователей и комплекса средств автоматизации.

- B) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных
технологий и технических средств
- C) Система, состоящая из АРМ, серверов и СКС
3. Информация - это:
- A) Сведения, полученные при исследовании, изучении или обучении
- B) Известия, новости, факты, данные
- C) Команды или символы представления данных (в системах связи или в компьютере)
- D) Знания (сообщения, экспериментальные данные, изображения), меняющие концепцию, полученную в
результате физического или умственного опыта
4. Что такое несанкционированный доступ?
- A) процесс обнаружения уязвимостей в программном обеспечении.
- B) Доступ, нарушающий правила разграничения доступа, изложенные в организационно-распорядительной
документации
- C) Доступ к информации, осуществляемый средствами, не входящими в состав автоматизированной системы
5. Является ли одним из базовых свойств безопасности:
- A) конфиденциальность
- B) неотрицание авторства
- C) доступность
- D) отчётность
6. Что такое информационный актив?
- A) субъект доступа
- B) информационный ресурс ограниченного доступа
- C) всё что имеет ценность для организации
7. Уязвимость это:
- A) Свойство системы
- B) совокупность условий и факторов, создающих потенциальную или реальную опасность
- C) слабость, которую можно использовать для нарушения системы или содержащейся в ней информации
- D) любое действие или связанная последовательность действий нарушителя
8. Угроза это:
- A) Свойство системы
- B) совокупность условий и факторов, создающих потенциальную или реальную опасность
- C) слабость, которую можно использовать для нарушения системы или содержащейся в ней информации
- D) любое действие или связанная последовательность действий нарушителя
9. Что такое "концепция информационной безопасности"?
- A) Совокупность норм и правил, регламентирующих взаимодействие пользователей и информационных ресурсов
- B) документ, описывающий общее видение вопросов информационной безопасности

- C) совокупность внутренних организационно-распорядительных документов по вопросам защиты информации

10. Как соотносятся технические требования и техническое задание

- A) Техническое задание - ГОСТированный документ, содержит технические требования
- B) Это одно и то же
- C) Технические требования включают в себя техническое задание

11. Что такое политика безопасности?

- A) Набор законов и подзаконных актов, регламентирующих процессы защиты информации
- B) Концептуальный документ, отражающий заинтересованность руководства в вопросах информационной
безопасности, и намерение что-либо предпринять
- C) Набор руководящих документов государственных ведомств.
- D) совокупность норм и правил обеспечения информационной безопасности

12. Регулятор вопросов защиты информации - это:

- A) орган исполнительной власти в пределах своей компетенции занимающийся вопросами защиты информации
- B) Любая организация, проводящая в жизнь свою политику безопасности
- C) Любая организация, в пределах своей компетенции занимающаяся вопросами защиты информации и
имеющая возможность влияния на решение таких вопросов

13. Гостехкомиссия и ФСТЭК это

- A) Гостехкомиссия - это отдел ФСТЭК, занимающийся вопросами защиты информации
- B) Гостехкомиссии сейчас не существует. правопреёмницей этой организации является ФСТЭК
- C) Две разных организации

14.Регуляторами вопросов информационной безопасности являются

- A) ФСТЭК
- B) ФСБ
- C) МВД
- D) Роскомнадзор
- E) Банк России

15. Входит ли в состав политики безопасности:

- A) Концепция информационной безопасности
- B) План мероприятий по разрешению аварийных ситуаций
- C) Пояснительная записка
- D) Проект должностной инструкции

16. К какой информации законодательство предписывает применять самые строгие меры по защите:

- A) конфиденциальной
- B) секретной
- C) коммерческой
- D) особой важности
- E) персональным данным

- F) совершенно секретной
17. Какой модели защиты информации не существует:
- A) дискреционной
- B) мандатной
- C) криптографической
- D) ролевой
18. К какой модели относится модель с произвольным управлением доступом субъектов к объектам, при котором
права доступа можно представить в виде матрицы субъект-объект:
- A) дискреционной
- B) мандатной
- C) криптографической
- D) ролевой
19. К какой модели относится модель с сопоставлением каждому объекту и субъекту классификационных меток,
отражающих их место в соответствующей иерархии:
- A) дискреционной
- B) мандатной
- C) криптографической
- D) ролевой
20. К какой модели относится модель, в которой, помимо матрицы доступа для субъектов-объектов, применяется
назначение пользователям определенных категорий:
- A) дискреционной
- B) мандатной
- C) криптографической
- D) ролевой
21. Какими свойствами не обладает информация, находящаяся в состоянии защищенности:
- A) конфиденциальности
- B) надежности
- C) целостности
- D) доступности
- E) отчетности
22. К какому типу нарушителя можно отнести лицо, получившее доступ в помещение с техническими средствами
АС:
- A) внешний
- B) злоумышленник
- C) внутренний
23. По какому признаку классифицируются нарушители в РД ГТК:
- A) по месту действия
- B) по достигаемым целям
- C) по уровню возможностей
- D) по характеру угроз
24. Комплекс организационно-технических мероприятий, в результате которых

подтверждается, что объект
соответствует требованиям стандартных или иных нормативно-технических документов по безопасности
информации, называется:
- A) исследование
- B) проверка
- C) аттестация
- D) рекомендация
- E) заключение

25. Под окном резервного копирования подразумевается
- A) скорость (время) восстановления из резервной копии
- B) скорость (время) резервного копирования в хранилище
- C) время простоя(отсутствия функционирования) системы по её прямому назначению
- D) накладные расходы: уровень нагрузки, создаваемой на сервер при выполнении копирования, уменьшение
скорости отклика сервиса

26. Регистрация событий позволяет решать следующие задачи:
- A) предоставление информации для выявления и анализа проблем
- B) обнаружение попыток нарушений
- C) обеспечение реконструкции последовательности событий
- D) реагирование на возникающие инциденты

27. Какие характеристики файлов могут быть использованы для контроля целостности:
- A) контрольная сумма файла
- B) хеш-функция
- C) время создания файла
- D) имитовставка файла

28. Какие модели не могут быть использованы без дополнительных моделей:
- A) мандатная
- B) ролевая
- C) криптографическая
- D) дискреционная

29. Хэш-функция является:
- A) обратимым преобразованием
- B) необратимым преобразованием
- C) случайным кодом

30. Чем является сетевая атака, приводящая к отказу в обслуживании
- A) сниффинг
- B) ip-спуффинг
- C) DoS
- D) парольной атакой
- E) атакой типа "Man-in-the-Middle"

3.3. Задания для промежуточной аттестации (зачета и (или) экзамена)

Список вопросов к зачету

1. Классификация автоматизированных систем (АС)
2. Информационные технологии, используемые в АС
3. Жизненный цикл АС
4. Основные угрозы безопасности информации в автоматизированных системах
5. Отказоустойчивость АС
6. Основные понятия и классификация защищенных автоматизированных систем
7. Понятия информации и информационных ресурсов. Предмет защиты информации
8. Понятие информационной безопасности
9. Понятие политики информационной безопасности
10. Понятие системы защиты информации. Основные положения безопасности автоматизированных систем
11. Трехэтапная разработка мер по обеспечению безопасности автоматизированных систем
12. Стадия выработки требований
13. Стадия определения способов защиты
14. Стадия определения функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты
15. Основные принципы обеспечения информационной безопасности в автоматизированной системе
16. Принципы, позволяющие реализовать положения по защите АС
17. Угрозы безопасности информации в защищенных автоматизированных системах
18. Базовые признаки угроз информационной безопасности. Классификация угроз
19. Уровни доступа к защищаемой информации
20. Подходы к обеспечению защиты информации. Сервисы безопасности
21. Виды аутентификации. Проблема надежной аутентификации и пути ее решения
22. Средства и методы хранения эталонных копий аутентификационной информации
23. Средства и методы защиты от компрометации и подбора паролей
24. Требования к защите компьютерной информации
25. Нормативные документы ФСТЭК, регламентирующие защиту информации от несанкционированного доступа
26. Основные подсистемы и группы механизмов защиты АС
27. Последовательность и содержание этапов разработки АС
28. Методы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем
29. Методы и средства обеспечения отказоустойчивости автоматизированных систем.
30. Критерии оценки защищенности АС
31. Методы обеспечения информационной безопасности АС. Организация коллективной разработки программного обеспечения АС
32. Проектирование защищенных АС. Основные методы проектирования
33. Основы ведения конструкторской документации
34. Структура и содержание технического задания
35. Построение комплексной защиты АС. Основы проектирования комплексной защиты информационной безопасности от НСД
36. Аттестация АС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации
37. Особенности эксплуатации АС на объекте защиты
38. Организация технического обслуживания защищенных АС

39. Аппаратно-программные средства диагностики АС
40. Протоколы аутентификации на прикладном уровне
41. Протоколы аутентификации на транспортном уровне
42. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI
43. Задачи администрирования подсистем АС. Средства администрирования АС
44. Настройка сетевой подсистемы защищенной АС
45. Принципы функционирования информационных сервисов АС
46. Установка и настройка работы информационных сервисов АС
47. Удаленное администрирование компонентов АС

Зачеты и экзамены могут быть проведены в письменной форме, а также в письменной форме с устным дополнением ответа. Зачеты служат формой проверки качества выполнения студентами лабораторных работ, усвоения семестрового учебного материала по дисциплине (модулю), практических и семинарских занятий (при отсутствии экзамена по дисциплине).

По итогам зачета, соответствии с модульно – рейтинговой системой университета, выставляются баллы с последующим переходом по шкале баллы – оценки за зачет, выставляемый как по наименованию «зачтено», «не зачтено», так и дифференцированно т.е. с выставлением отметки по схеме – «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно», определяемое решением Ученого совета университета и прописываемого в учебном плане.

Экзамен по дисциплине (модулю) служит для оценки работы студента в течении семестра (года, всего срока обучения и др.) и призван выявить уровень, качество и систематичность полученных им теоретических и практических знаний, приобретения навыков самостоятельной работы, развития творческого мышления, умения синтезировать полученные знания и применять их в решении практических задач. По итогам экзамена, в соответствии с модульно – рейтинговой системой университета выставляются баллы, с последующим переходом по шкале оценок на оценки: «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно», свидетельствующие о приобретенных компетенциях или их отсутствии.

В ФОС размещается пример заполненного экзаменационного билета. Весь комплект экзаменационных билетов по дисциплине хранится на кафедре в соответствии с утвержденной номенклатурой дел.

Критерии оценки уровня сформированности компетенций по результатам проведения зачета:

- оценка «зачтено»: обучающийся демонстрирует всестороннее, систематическое и глубокое знание материала, свободно выполняет задания, предусмотренные программой дисциплины, усвоивший основную и дополнительную литературу. Обучающийся выполняет задания, предусмотренные программой дисциплины, на уровне не ниже базового;
- оценка «не зачтено»: обучающийся демонстрирует незнание материала, не выполняет задания, предусмотренные программой дисциплины. Обучающийся не выполняет задания, предусмотренные программой дисциплины, на уровне ниже базового. Дальнейшее освоение ОПОП не возможно без дополнительного изучения материала и подготовки к зачету.

Критерии оценки уровня сформированности компетенций по результатам проведения дифференцированного зачёта (зачета с оценкой) / экзамена:

- оценка **«отлично»:** обучающийся дал полный, развернутый ответ на поставленный вопрос, проявил совокупность осознанных знаний об объекте, доказательно раскрыл основные положения темы. В ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, явлений. Обучающийся

подкрепляет теоретический ответ практическими примерами. Ответ сформулирован научным языком, обоснована авторская позиция обучающегося. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа или с помощью «наводящих» вопросов преподавателя. Обучающимся продемонстрирован высокий уровень владения компетенцией(-ями);

- оценка **«хорошо»:** обучающимся дан полный, развернутый ответ на поставленный вопрос, проявлено умение выделять существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, но есть недочеты в формулировании понятий, решении задач. При ответах на дополнительные вопросы допущены незначительные ошибки. Обучающимся продемонстрирован повышенный уровень владения компетенцией(-ями);

- оценка **«удовлетворительно»:** обучающимся дан неполный ответ на вопрос, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, явлений, нарушена логика ответа, не сделаны выводы. Речевое оформление требует коррекции. Обучающийся испытывает затруднение при ответе на дополнительные вопросы. Обучающимся продемонстрирован базовый уровень владения компетенцией(-ями);

- оценки **«неудовлетворительно»:** обучающийся испытывает значительные трудности в ответе на вопрос, допускает существенные ошибки, не владеет терминологией, не знает основных понятий, не может ответить на «наводящие» вопросы преподавателя. Обучающимся продемонстрирован низкий уровень владения компетенцией(-ями).