МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Первый проректор
_____ А.В. Толстиков
24 марта 2022 г.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ
МОДЕЛИ И МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ СИСТЕМ
по научной специальности
2.3.6. Методы и системы защиты информации, информационная безопасность

1. Паспорт оценочных материалов по дисциплине

№ п/п	Темы дисциплины (модуля) в ходе текущего контроля, вид промежуточной аттестации (зачет, с указанием семестра)	Код и содержание компетенции	Оценочные материалы *(виды и количество)*
1	2	3	4
1.	Классификация угроз информационной безопасности	ПК-2 - способность к разработке и реализации принципов и решений (технических, математических, организационных и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования; ПК-9 - способность к созданию новых и совершенствованию существующих моделей и методов оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты вне зависимости от области их функционирования; ПК-14 - готовность к проведению комплексных исследований научных и технических проблем с применением математического моделирования, вычислительного эксперимента и программных средств.	Устный опрос.
2.	Нормативно-правовой подход к обеспечению информационной безопасности		Устный опрос.
3.	Практический (экспериментальный) подход к обеспечению информационной безопасности		Устный опрос.
4	Определение и разработка политики безопасности		Устный опрос.
5.	Аудит информационной безопасности		Устный опрос.
6.	Дифференцированный зачет (4 семестр)		Вопросы к дифференцированному зачету.

2. Виды и характеристика оценочных средств

Устный опрос проводится по теоретическому материалу. Для подготовки необходимо проработать лекцию и прочитать рекомендуемую литературу по теме. Устный опрос может проводиться в форме индивидуального собеседования или собеседования в малых группах по вопросам.

Дифференцированный зачет проводится в форме собеседования по билетам с заранее распределёнными вопросами. Собеседование имеет целью выявление уровня освоения дисциплины, характеризующего знания обучающегося в соответствии с определенными компетенциями.

3. Оценочные средства

Примеры средств для проведения текущего контроля

3.1. Устный опрос

Проводится по теоретическому материалу. Для подготовки необходимо проработать лекцию и прочитать рекомендуемую литературу по теме. Устный опрос может проводиться в форме индивидуального собеседования или собеседования в малых группах по вопросам.

Пример.

Собеседование по теме 1. *Классификация угроз информационной безопасности.*

1. Дайте определение информационной безопасности.
2. Назовите модели угроз и охарактеризуйте антропогенные виды угроз.
3. Опишите модель нарушителя: определение хакерства. Цели и задачи хакера.

3.2. Дифференцированный зачет

Дифференцированный зачет проводится по билетам, содержащим по 2 вопроса (теоретический и прикладной).

Теоретические вопросы формулируются по тематике лекций.

Прикладные вопросы связаны с соответствующими теоретическими и основаны на материале практических занятий по дисциплине и диссертационного исследования аспиранта.

Оценка **«отлично»** ставится при соблюдении следующих условий:

- грамотное и правильное использование в ответах специальной и общенаучной терминологии;
- безошибочное владение категориальным аппаратом научного направления;
- умение обозначить основные проблемы сформулированных в билетах вопросов;
- безошибочное знание фактического материала;
- умение связать ответ на вопрос с темой диссертационного исследования;
- логичность, связность ответа.

Оценка **«хорошо»** ставится при соблюдении следующих условий:

- грамотное использование в ответах специальной и общенаучной терминологии;
- проблемное изложение ответов на сформулированные в билетах вопросы;
- отдельные ошибки при изложении фактического материала;
- умение связать ответ на вопрос с темой диссертационного исследования;
- логичность, связность ответа.

Оценка **«удовлетворительно»** ставится за:

- недостаточное использование в ответах специальной и общенаучной терминологии;
- недостаточное владение категориальным аппаратом отрасли науки;
- умение обозначить только одну из проблем, сформулированных в билетах вопросов;
- ошибки при изложении фактического материала;
- нарушение логичности и связности ответа.

Оценка **«неудовлетворительно»** ставится за:

- отсутствие в ответах необходимой специальной и общенаучной терминологии;
- описательное изложение ответов на сформулированные в билетах вопросы, неумение обозначить и изложить проблемы;
- грубые ошибки при изложении фактического материала;
- неумение связать ответ на вопрос с темой диссертационного исследования;
- нарушение логичности, связности ответа.

Вопросы к дифференцированному зачету

1) Определение информационной безопасности (ИБ). Определение конфиденциальности, целостности и доступности. Основные подходы к обеспечению ИБ.

2) Определение «уязвимости», «угрозы», «атаки» и «эксплойта». Модели угроз и виды угроз (антропогенные, техногенные, стихийные источники угроз).

3) Модель нарушителя: определение хакерства. Цели и задачи хакера. «Белые», «серые» и «черные» хакеры. Социальная инженерия: определение, задачи, примеры применения для нарушения конфиденциальности, целостности и доступности информации.

4) Основные механизмы обеспечения ИБ: идентификация, аутентификация, авторизация, аудит.

5) Парольные системы аутентификации. Стойкость парольных систем аутентификации. Взаимная проверка подлинности пользователей информационной системы.

6) Биометрические системы аутентификации. Основные методы взлома биометрических систем аутентификации.

7) Основные модели разграничения прав доступа: дискреционная, мандатная и ролевая модели доступа.

8) Криптографическая защита информации: определение шифрования, расшифрования, дешифрования, криптографического ключа, хеширования информации.

9) Симметричное и асимметричное шифрование. Примеры симметричного и асимметричного шифрования: шифр Виженера, алгоритм RSA.

10) Электронно-цифровая подпись (ЭЦП): определение ЭЦП, схема ЭЦП, определение сертификата открытого ключа, удостоверяющего центра. Инфраструктура открытых ключей (PKI).

11) Кодирование информации как средство обеспечения целостности информации. Примеры алгоритмов кодирования.

12) Стеганография как один из способов обеспечения конфиденциальности и целостности информации.

13) Формальные модели безопасности информационных систем (ИС): обобщенные модели систем защиты ИС; вероятностные модели систем защиты информации ИС; модели безопасности ИС, построенные с использованием теории графов; модели безопасности ИС, построенные с использованием теории автоматов.

14) Эталонные модели взаимодействия открытых ИС: TCP/IP и OSI. Структура моделей. Уязвимости канального уровня.

15) Эталонные модели взаимодействия открытых ИС: TCP/IP и OSI. Структура моделей. Уязвимости сетевого уровня.

16) Эталонные модели взаимодействия открытых ИС: TCP/IP и OSI. Структура моделей. Уязвимости транспортного уровня.

17) Эталонные модели взаимодействия открытых ИС: TCP/IP и OSI. Структура моделей. Уязвимости прикладного уровня.

18) Нормативный подход в обеспечении ИБ. Политика безопасности (ПБ), модель ПБ. Оранжевая книга, классы безопасности ИС.

19) Аспекты защиты интеллектуальной собственности. Проблемы «пиратства». Реверсивный инжиниринг (обратное проектирование): цели, задачи, основные методы.

20) Алгоритм оценки и анализа рисков безопасности ИС. Управление рисками безопасности ИС.

21) Технические каналы утечки информации: акустический и виброакустический каналы; оптический канал утечки; электромагнитный канал утечки информации, ПЭМИН; материальный канал утечки информации. Основные способы защиты от утечки.

22) Организационные, технические и режимные меры обеспечения информационной безопасности информационных систем.

23) Определение «вируса». Структура «вируса». Принцип работы антивирусных программ. Обфускация (запутывание программного кода) и деобфускация.

24) Атака типа «отказ в обслуживании»: DoS, DDoS. Принцип построения «зомби»-сетей, основные цели атаки. Доступность как одно из ключевых свойств информации.