

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Поверинов Игорь Егорович

Должность: Проректор по учебной работе

Дата подписания: 25.12.2024 09:24:05

Уникальный программный ключ:

6d465b936eef331cede482bded6d124078218052f016469873871a2eab0de1b2

МИНОБРНАУКИ РОССИИ

**Федеральное государственное бюджетное образовательное учреждение
высшего образования**

«Чувашский государственный университет имени И.Н. Ульянова»

(ФГБОУ ВО «ЧГУ им. И.Н. Ульянова»)

Факультет информатики и вычислительной техники

Кафедра математического и аппаратного обеспечения информационных систем

УТВЕРЖДЕНЫ

на заседании кафедры

05 ноября 2024 г., протокол № 4

Заведующий кафедрой

Т.Н. Копышева

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине (модулю)

«Математическое моделирование процессов защиты информации»

Научная специальность – 2.3.6. Методы и системы защиты информации,
информационная безопасность

Форма обучения – очная

Год начала освоения – 2022

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

Заведующий кафедрой математического
и аппаратного обеспечения
информационных систем, к.ф.-м.н., доцент
Т.Н. Копышева

СОГЛАСОВАНО:

Декан факультета А.В. Щипцова

1. Паспорт оценочных материалов по дисциплине (модулю).

№ п/п	Контролируемые разделы (темы) дисциплины	Контролируемые результаты освоения дисциплины (модуля)	Наименование оценочного средства
Семестр 4			
Раздел 1. Основные модели информационной безопасности			
1.	Тема 1. Основы моделирования в информационной безопасности	К4, К7	Устный опрос на практических занятиях, вопросы к зачету.
2.	Тема 2. Основные модели информационной безопасности	К4, К7	Устный опрос на практических занятиях, вопросы к зачету.
Раздел 2. Современные подходы к моделированию информационной безопасности			
3.	Тема 3. Модели оценки средств защиты информации	К4, К7	Устный опрос на практических занятиях, вопросы к зачету.
4.	Тема 4. Моделирование нейросетевых средств защиты	К4, К7	Устный опрос на практических занятиях, вопросы к зачету.

В процессе освоения данной дисциплины, обучающиеся формируют следующие результаты освоения дисциплины:

К4 – способность самостоятельно осуществлять научно-исследовательскую деятельность в соответствующей профессиональной области с использованием современных методов исследования;

К7 - способность к разработке научных основ, принципиально новых методов анализа и синтеза, научных подходов и технических принципов создания систем защиты информации и информационной безопасности.

2. Критерии оценки успеваемости обучающихся.

Критерии получения зачета по дисциплине:

Оценка «зачтено» ставится:

- если аспирант глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, не затрудняется с ответом при видоизменении задания, свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, умеет самостоятельно обобщать и излагать материал, не допуская ошибок;

- если аспирант твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми умениями и навыками при выполнении практических заданий;

- если аспирант усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий.

Зачет считается не сданным, если аспирант не знает отдельных разделов программного материала, допускает существенные ошибки, с большими затруднениями выполняет, либо не может самостоятельно выполнить практические задания.

3. Оценочные материалы текущего контроля успеваемости.

3.1. Примерный перечень вопросов для устного опроса.

1. Математические основы моделей безопасности. Теория автоматов
2. Математические основы моделей безопасности. Теория графов
3. Математические основы моделей безопасности. Классы алгоритмических задач
4. Математические основы моделей безопасности. Классификация моделей информационной безопасности
5. Модель матрицы доступов
6. Модель распространения прав доступа
7. Модели систем мандатного разграничения доступа
8. Модель Белла-ЛаПадула, Биба
9. Безопасность переходов
10. Модель систем военных сообщений
11. Модели ролевого разграничения доступа
12. Базовая модель РРД
13. Администрирование РРД
14. Механизм мандатного контроля в РРД
15. Модели безопасности информационных потоков
16. Автоматная модель безопасности
17. Контроль информационных потоков
18. Вероятностная модель
19. Выявление скрытых каналов
20. Изолированная программная среда
21. Монитор безопасности объектов
22. Изолированная программная среда
23. Доверенные системы
24. Основные понятия и принципы средств защиты информации
25. Функциональные требования средств защиты информации
26. Оценочные критерии средств защиты информации
27. Нейросетевые модели средств защиты
28. Распознавание и классификация событий
29. Выявление аномалий в рядах данных

Критерии оценки устного опроса

Развернутый ответ должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения, правила в конкретных случаях. Критериями оценивания являются:

- 1) полнота и правильность ответа;
- 2) степень осознанности, понимания изученного;
- 3) языковое оформление ответа.

Оценка «зачтено» ставится, если обучающийся полно излагает материал, дает правильное определение основных понятий, обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры, излагает материал последовательно и правильно с точки зрения норм литературного языка.

Оценка «не зачтено» ставится, если обучающийся обнаруживает незнание большей части соответствующего вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, неуверенно излагает материал. Оценка «не зачтено» отмечает такие недостатки в подготовке, которые являются серьезным препятствием к успешному овладению последующим материалом.

4. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины (модуля).

4.1. Примерный перечень вопросов к зачету

1. Понятия и концепции моделирования как метода научного познания.
2. Экспериментальный подход к моделированию.
3. Аналитический и численный подходы к моделированию.
4. Информационный подход к моделированию. Современные тенденции.
5. Наука о данных – Data Science. История возникновения и основы.
6. Терминология и методы Науки о данных.
7. Диаграмма Венна, варианты диаграммы Венна
8. Методы интеллектуального анализа и моделирования данных.
9. Интеллектуальный анализ данных как основная составляющая науки о данных и информационного подхода к моделированию
10. Методы предобработки данных (очистка, фильтрация, парциальная обработка)
11. Методы предварительного анализа данных (факторный и корреляционный анализы)
12. Методы моделирования данных (линейная и логистическая регрессия).
13. Искусственные нейронные сети как метод моделирования процессов защиты информации.
14. Искусственные нейронные сети. История и теоретические основы искусственных нейронных сетей.
15. Практические основы применения искусственных нейронных сетей.
16. Технологии и методики применения аналитических платформ в моделировании.
17. Обзор существующих аналитических платформ
18. Технологии и методики применения различных аналитических платформ.
19. Практические основы применения аналитических платформ.
20. Примеры применения аналитических платформ при моделировании процессов защиты информации.
21. Перспективные задачи моделирования процессов защиты информации.
22. Постановка задачи моделирования процессов защиты информации.
23. Математические основы моделей безопасности. Классификация моделей информационной безопасности