

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 28.07.2025 09:33:11
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

УТВЕРЖДЕНО

на заседании высшей школы

интеллектуальных систем и
кибертехнологий

Протокол от 15.12.2023 № 4

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

(фонд оценочных средств)

для проведения промежуточной аттестации по дисциплине

«Моделирование защищённых автоматизированных систем»

наименование дисциплины

по образовательной программе высшего образования – программе

магистратуры

бакалавриата, специалитета,
магистратуры

«Информационная безопасность интеллектуальных и информационно-аналитических систем»

наименование образовательной программы

10.04.01 «Информационная безопасность»

шифр, наименование направления подготовки / специальности

Составитель

Глухова Л.В. профессор, высшая школа
интеллектуальных систем и кибертехнологий,
д.э.н., профессор

ФИО, должность, структурное подразделение,
ученая степень, ученое звание

Тольятти
2023

1. Паспорт фонда оценочных средств

1.1. Планируемые результаты обучения по дисциплине

Код компетенции	Наименование компетенции	Код и наименование индикаторов достижения компетенции
ОПК-2.	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ИОПК-2.3. Разрабатывает технические проекты защищённых информационных систем
ПК-4.	Способен разработать архитектуру системы защиты информации и провести анализ уязвимости и эффективности её модели с учетом специфики деятельности организации и обрабатываемых данных	ИПК-4.1. Исследует программные и архитектурно-технические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в них, опираясь на математическое моделирование; ИПК-4.2. Применяет математические модели при проектировании систем защиты информации, в частности интеллектуальных и информационно-аналитических систем

В результате изучения дисциплины обучающийся должен:

владеть навыками:

- разработки архитектуры систем защиты информации, используя математический аппарат нейро-нечеткой логики и программные средства;
- поэтапного решения задач профессиональной деятельности;

уметь:

- применять математические модели интеллектуальных и информационно-аналитических систем при проектировании систем защиты информации;
- применять современные интеллектуальные и информационные технологии и стандарты проектирования при разработке технического проекта защищенных информационных систем;

знать:

- аппарат нейро-нечеткой логики и тензорного анализа;
- известные программные и архитектурно-технические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в них, опираясь на математическое моделирование;
- требования ТЗ к разработке проекта защищенной информационной системы.

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Компетенция
1	Тема 1. Интеллектуальные средства и методы математического моделирования систем защиты информации в соответствии с требованиями ТЗ	ОПК-2
2	Тема 2. Математическое моделирование систем защиты информации и оценки их защищенности. Разработка адаптивной модели системы защиты информации	ПК-4
3	Тема 3. Аспекты организации адаптивных систем защиты информации на базе логарифмической структурной модели формального нейрона	ПК-4 ОПК-2

1.3. Система оценивания по дисциплине

Дисциплина изучается в течение одного семестра.
Форма промежуточной аттестации по дисциплине – экзамен.

Шкала оценки уровня сформированности компетенций		Шкала оценки уровня освоения дисциплины	
Уровневая шкала оценки компетенций	100 балльная шкала, %	100 балльная шкала, %	5-балльная шкала, дифференцированная оценка/балл
Допороговый	Ниже 61	Ниже 61	«Неудовлетворительно» / 2
Пороговый	61-85,9	61-69,9	«Удовлетворительно» / 3
		70-85,9	«Хорошо» / 4
Повышенный	86-100	86-100	«Отлично» / 5

2. Перечень оценочных материалов для проведения промежуточной аттестации

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в ходе текущего контроля успеваемости (в процессе проведения практических занятий, тестирования, опросов).

В ходе проведения промежуточной аттестации осуществляется контроль и оценка результатов освоения компетенций.

Перечень вопросов для подготовки к экзамену

ПК-4: ИПК-4.1, ИПК-4.2. Способен разработать архитектуру системы защиты информации и провести анализ уязвимости и эффективности её модели с учетом специфики деятельности организации и обрабатываемых данных

1. Какая деятельность должна быть выявлена для обнаружения аномалий при раскрытии потенциальных уязвимостей безопасности информации
2. В чем особенность метода обучения нейронных сетей с названием «метод обратного распространения»?
3. Что понимается под весом в нейронной сети?
4. Перечислить наиболее часто используемые методы обучения нейронных сетей, по вашему мнению
5. Сформулировать понятие интеллектуальной системы и ее базовой структуры.
6. Сформулировать понятие информационно-аналитической системы и привести ее пример.
7. Сформулировать, что понимается под методом машинного обучения
8. Навыки разработки архитектуры систем защиты информации могут быть сформированы методами разработки математических моделей на основе использования математического аппарата нечетких систем в программе *MATLAB7.0.1*. Описать основные возможности пакета *MATLAB7.0.1*
9. Описать сущность методики экспертной оценки защищенности систем информационных технологий
10. Связующим звеном адаптивной модели СЗИ является методика оценки защищенности ИТ-системы. Описать ее основное назначение
11. Опишите особенности систем защиты информации для обнаружения атак
12. Какие основные компоненты входят в структуру нейронной сети?
13. Сформулировать понятие ИТ-инфраструктура
14. Наиболее распространенные разновидности вредоносных программ, используемых для кибератак, и их краткая характеристика, которую должен учесть разработчик при проектировании систем защиты ИБ(перечислить разновидности компьютерных вирусов)
15. Перечислить разновидности вредоносных утилит, не менее 3-х, которые используются злоумышленниками для кибератак

ОПК-2: ИОПК-2.3. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности

1. Назначение и характеристика ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения»
2. Каким образом формируется набор индикаторов компрометации, используемый при осуществлении мониторинга?
3. Сколько уровней защиты информации установлено ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер»? Дайте их характеристику при использовании в целях обеспечения соответствия уровням защищенности персональных данных
4. Назначение и характеристика ГОСТ Р 51583—2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»

5. Опишите этапы работ стадии «Технический проект» в соответствии с ГОСТ 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»

6. Каковы составляющие методологии построенной на идеях тензорного анализа Крона

7. Что понимается под системно-аналитическими исследованиями?

8. Дайте определение тензора и его математическое описание

9. В чем заключается и что позволяет третья фундаментальная идея тензорного анализа Крона?

10. Опишите, из каких этапов состоит стадия «реагирование на компьютерные инциденты» (по ГОСТ 59712-2022)