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 | **Основание (ПС)** \*для профессиональных компетенций |
| 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 | ПС 06.033 Специалист по защите информации в автоматизированных системах |

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 логикии 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 | Индикатор достижения компетенции |
| 1 | Тема 1. Интеллектуальные средства и методы математического моделирования систем защиты информациив соответствии с требованиями ТЗ | ОПК-2 | ИОПК-2.3 |
| 2 | Тема 2.Математическое моделирование систем защиты информации и оценки их защищенности. Разработка адаптивной модели системы защиты информации | ПК-4 | ИПК-4.1  ИПК-4.2 |
| 3 | Тема 3. Аспекты организации адаптивных систем защиты информации на базе логарифмической структурной модели формального нейрона | ПК-4  ОПК-2 | ИПК-4.1  ИПК-4.2  ИОПК-2.3 |

**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 *MATLAB*7.0.1. Описать основные возможности пакета *MATLAB*7.0.1
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 вредоносныхпрограмм, 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)

**Вопросы (задания) для подготовки к зачету (экзамену)**

**с «ключами» правильных ответов**

| № | | Содержание вопроса | Правильный ответ |
| --- | --- | --- | --- |
| **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** | | | | |
|  | | Какая деятельность должна быть выявлена для обнаружения аномалий при раскрытии потенциальных уязвимостей безопасности информации | Для обнаружения аномалий выявляется деятельность, которая: 1) отличается от шаблонов, установленных для пользователей или групп пользователей;  2) связана с созданием базы данных;  3) содержит профили контролируемой деятельности |
|  | | В чем особенность метода обучения нейронных сетей с названием «метод обратного распространения»? | Метод обратного распространения состоит в следующем. Когда нейронная сеть делает предсказание, оно сравнивается с реальным результатом, и если есть ошибка, то веса в сети корректируются, чтобы уменьшить данную ошибку |
|  | | Что понимается под весом в нейронной сети? | Под весом в нейронной сети понимаются числовые значения, которые определяют, как сильно входные сигналы влияют на выходной результат |
|  | | Перечислить наиболее часто используемые методы обучения нейронных сетей, по вашему мнению | Существует несколько методов обучения нейронных сетей, но, по нашему мнению, наиболее часто применяются 3 метода:  Метод обратного распространения  Метод упругого распространения Генетический Алгоритм |
|  | | Сформулировать понятие интеллектуальной системы и ее базовой структуры. | Под интеллектуальной системой понимается система, основанная на знаниях, или комплекс программных, лингвистических и логико-математических средств для реализации основной задачи – осуществления поддержки деятельности человека и поиска информации в режиме продвинутого диалога на естественном языке.  Ее структура имеет вид: база знаний; решатель; интеллектуальный интерфейс, позволяющий вести общение с ЭВМ без специальных программ для ввода данных |
|  | | Сформулировать понятие информационно-аналитической системы и привести ее пример. | Информационно-аналитическая система – это комплекс технических и программных средств для сбора, хранения, обработки и анализа больших объемов данных, необходимых для принятия стратегических, тактических и оперативных решений  Например, Альт Инвест может быть использована как инструмент информационно-аналитической деятельности. С ее помощью может быть выполнена экспертиза инвестиционных проектов и разработка бизнес-планов |
|  | | Сформулировать, что понимается под методом машинного обучения | Методы машинного обучения — это класс методов искусственного интеллекта, характерной чертой которых  является не прямое решение задачи, а обучение за счет применения решений множества сходных задач |
|  | | Навыки разработки архитектуры систем защиты информации могут быть сформированы методами разработки математических моделей на основе использования математического аппарата нечетких систем в программе *MATLAB*7.0.1. Описать основные возможности пакета *MATLAB*7.0.1 | 1. определение переменных, нечетких правил и функций принадлежности; 2. интерактивный просмотр нечеткого логического вывода; 3. адаптивный нечеткий вывод с использованием нейронных сетей, нечеткая кластеризация;   интерактивное динамическое моделирование в *Simulink* |
|  | | Описать сущность методики экспертной оценки защищенности систем информационных технологий | Экспертная методика состоит из 4-х шагов:   1. Получение экспертных оценок. 2. Сближение мнений экспертов и корректировка результатов экспертизы. 3. Вычисление экспертной оценки проекта по локальным показателям. 4. Задаемся весом каждой градации, она позволяет получить оценки локальных показателей безопасности для защищенной автоматизированной системы |
|  | | Связующим звеном адаптивной модели СЗИ является методика оценки защищенности ИТ-системы. Описать ее основное назначение | Основное назначение методики оценки защищенности ИТ-системы состоит в следующем:   1. координирует взаимосвязь классификаторов угроз и механизмов защиты; 2. представляет взаимосвязь классификаторов угроз и механизмов защиты в виде нейронной сети, нечетких нейронных сетей, систем нечетких предикатных правил; 3. описывает взаимосвязь классификаторов угроз и механизмов защиты в виде структурной модели системы информационной безопасности; 4. обосновывает выбор инструментальных средств взаимосвязи классификаторов угроз и механизмов защиты путем расчета показателей защищенности и рейтинга ИТ-системы |
|  | | Опишите особенности систем защиты информации для обнаружения атак | Для обнаружения атак применяют системы защиты информации, в качестве интеллектуального инструмента в которых, как правило, используются нейронные сети, системы нечеткой логики и основанные на правилах экспертные системы |
|  | | Какие основные компоненты входят в структуру нейронной сети | Основные компоненты входящие в структуру нейронной сети: входы, веса и функция активации. Каждый нейрон принимает значения от предыдущих слоев умножает их на соответствующие веса и передает результат в функцию активации, которая определяет: активируется нейрон или нет |
|  | | Сформулировать понятие ИТ-инфраструктура | ИТ-инфраструктура – это совокупность программных сервисов, служб, аппаратных средств и корпоративных документов, обеспечивающих возможности создания, хранения, передачи, обработки, защиты и удаления информации в пределах отдельной организации или системы организаций |
|  | | 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) | Наиболее распространенными разновидностями вредоносных программ являются: файловые вирусы, загрузочные вирусы, макровирусы |
|  | | Перечислить разновидности вредоносных утилит, не менее 3-х, которые используются злоумышленниками для кибератак | Наиболее распространенные разновидности вредоносных программ, используемых для кибератак, которые должен учесть разработчик при проектировании систем защиты ИБ, это Constructor, HackTool,Spoofer |
| **ОПК-2:** **ИОПК-2.3. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности** | | | | |
|  | Назначение и характеристика ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения» | | ГОСТ Р 59547-2021«Защита информации. Мониторинг информационной безопасности. Общие положения» разработан Федеральной службой по техническому и экспортному контролю (ФСТЭК России). В документе описаны сведения о процесс постоянного наблюдения и анализа результатов регистрации событий безопасности. Документ позволяет выполнять мониторинг информационной безопасности |
|  | Каким образом формируется набор индикаторов компрометации, используемый при осуществлении мониторинга? | | Используемый при осуществлении мониторинга набор индикаторов компрометации берется из источника, распространяющего сведения о выявленных индикаторах компрометации.  Набор индикаторов компрометации  формируется как поток данных об угрозах, содержащий индикаторы компрометации |
|  | 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 | | ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер» определяет три уровня защиты информации. В порядке значимости их можно расположить следующим образом:  уровень 3 – минимальный,  уровень 2 – стандартный,  уровень 1 - усиленный  Для обеспечения соответствия четвертому уровню защищенности персональных данных при их обработке в ИСПДн, установленных Правительством Российской Федерации, рекомендуется использовать требования, установленные ГОСТ Р 57580.1-2017, уровень 3 – минимальный.  Для обеспечения соответствия третьему и второму уровням защищенности персональных данных – уровень 3 – минимальный  Для обеспечения соответствия первому уровню защищенности персональных - уровень 1 - усиленный |
|  | Назначение и характеристика ГОСТ Р 51583—2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» | | ГОСТ Р 51583—2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» описывает порядок создания автоматизированных систем в защищенном исполнении.  Создание системы защиты информации в автоматизированной системе защиты информации (АСЗИ) в соответствии с ГОСТ Р 51583-2014 обеспечивается следующим комплексом работ:  - формирование требований к системе ЗИ АСЗИ;  - разработка (проектирование) системы ЗИ АСЗИ;  - внедрение системы ЗИ АСЗИ;  - аттестация АСЗИ на соответствие требованиям безопасности информации и ввод ее в действие;  - сопровождение системы ЗИ в ходе эксплуатации АСЗИ |
|  | Опишите этапы работ стадии «Технический проект» в соответствии с ГОСТ 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» | | На стадии «Технический проект» в интересах создания системы ЗИ создаваемой (модернизируемой) АСЗИ в соответствии с ГОСТ 51583-2014 (акт.2018) «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» выполняют следующие работы:   * Этап: Разработка проектных решений по системе и ее частям; * Этап: Разработка документации на АС и ее части; * Этап: Разработка и оформление документации на поставку изделий для комплектования АС и (или) технических требований (технических заданий) на их разработку; * Этап: Разработка заданий на проектирование в смежных частях проекта объекта информатизации |
|  | Каковы составляющие методологии построенной на идеях тензорного анализа Крона | | К эти составляющим относятся:  1) способы расчленения (декомпозиции) сложносоставных систем на части и их исследования (расчета) по частям;  2) способы объединения (композиции)  частных результатов с целью синтеза решения для системы в целом |
|  | .Что понимается под системно-аналитическими исследованиями? | | Отношения, взаимодействия и связи представляют собой различаемые по формальному признаку, но взаимно образующие и взаимно обусловливающие категории, образующие предметный базис (по Крону) |
|  | Дайте определение тензора и его математическое описание | | Тензор определяется как геометрический объект, который описывается многомерным массивом, то есть набором чисел,  занумерованных несколькими индексами, или, иначе говоря,**n**-мерной таблицей, где ***п*** - валентность тензора |
|  | В чем заключается и что позволяет третья фундаментальная идея тензорного анализа Крона? | | Третья фундаментальная идея тензорного анализа Крона заключается в том, чтобы закодировать как все дискретные элементы пространства, в котором ведется анализ, так и системы функций, «привязанных» к каждой точке этого пространства. Это позволяет унифицировать параметры и дать однообразные  описания весьма разнообразным частям, образующим сложную систему. |
|  | Опишите, из каких этапов состоит стадия «реагирование на компьютерные инциденты» (по ГОСТ 59712-2022) | | Стадия «реагирование на компьютерные инциденты» (по ГОСТ 59712-2022­) состоит из следующих последовательных этапов:  - определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры;  - локализация компьютерного инцидента;  - выявление последствий компьютерного инцидента;  - ликвидацияпоследствий компьютерного инцидента;  - закрытие компьютерного инцидента |