Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.04.01 Информационная безопасность

Наименование образовательной программы: Управление информационной безопасностью

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Оценочные материалы
по дисциплине
Интеллектуальный анализ данных и процессов

Москва
2023

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Минзов А.С. Идентификатор: R17801759-MinzovAS-e8de8907	А.С. Минзов
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Минзов А.С. Идентификатор: R17801759-MinzovAS-e8de8907	А.С. Минзов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ПК-1 Оценивание уровня безопасности компьютерных систем и сетей
   ПК-1.5 Проводит инструментальный мониторинг защищенности компьютерных систем и сетей

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

1. Контрольное задание № 1. Классификация задач, решение которых целесообразно с использованием экспертных систем. Контрольное задание № 2. Принципы, методы, технологии и средства извлечения знаний методами Data Mining с использованием деревьев решений. (Контрольная работа)
2. Контрольное задание № 3. Практическое задание по использованию статистического метода обработки данных большого объема BigDate. 4. Контрольное задание № 4. Разработка систем проактивной информационной без-опасности на основе анализа событий в информационной системе. (Контрольная работа)
3. Контрольное задание № 5. Практическое задание по использованию технологии Data Mining (Контрольная работа)
4. Контрольное задание № 6. Методы и технологии применения ИТ экспертных систем в про-фессиональной деятельности (Контрольная работа)

БРС дисциплины

1 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Технологии и средства интеллектуального анализа					
Термины и определения		+	+		
Теоретические основы техно-логий интеллектуального анализа и экспертных систем для оценки безопасности ИС					
Статистические методы обработки данных большого объема (BigDate): корреляционный, кластерный и регрессионный анализ		+	+		+
Практическое применение технологии Data Mining и экспертных систем					
Практическое использование технологии Data Mining и оболочек экспертных систем			+	+	

Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ПК-1	ПК-1.5$_{ПК-1}$ Проводит инструментальный мониторинг защищенности компьютерных систем и сетей	Знать: статистические методы обработки данных большого объема принципы, методы, технологии и средства извлечения знаний методами Data Mining с использованием деревьев решений классификацию технологий интеллектуального анализа данных и классификацию задач, при решении которых целесообразно с использованием технологий интеллектуального анализа данных и методов искусственного интеллекта Уметь: применять методы и технологии применения ИТ экспертных систем в	Контрольное задание № 1. Классификация задач, решение которых целесообразно с использованием экспертных систем. Контрольное задание № 2. Принципы, методы, технологии и средства извлечения знаний методами Data Mining с использованием деревьев решений. (Контрольная работа) Контрольное задание № 3. Практическое задание по использованию статистического метода обработки данных большого объема BigDate. 4. Контрольное задание № 4. Разработка систем проактивной информационной без-опасности на основе анализа событий в информационной системе. (Контрольная работа) Контрольное задание № 5. Практическое задание по использованию технологии Data Mining (Контрольная работа) Контрольное задание № 6. Методы и технологии применения ИТ экспертных систем в про-фессиональной деятельности (Контрольная работа)

		профессиональной деятельности разрабатывать систему проактивной информационной безопасности на основе анализа событий в информационной системе использовать технологию Data Mining и оболочки экспертных систем на практике	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контрольное задание № 1. Классификация задач, решение которых целесообразно с использованием экспертных систем. Контрольное задание № 2. Принципы, методы, технологии и средства извлечения знаний методами Data Mining с использованием деревьев решений.

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Контрольное мероприятие проводится в письменной форме

Краткое содержание задания:
Принципы, методы, технологии и средства извлечения знаний методами Data Mining с использованием деревьев решений.
Используя материалы, опубликованные в сети Интернет, а также рекомендованную учебную литературу ответить на следующие вопросы

Контрольные вопросы/задания:

Знать: классификацию технологий интеллектуального анализа данных и классификацию задач, при решении которых целесообразно с использованием технологий интеллектуального анализа данных и методов искусственного интеллекта	1.3. В чем заключается интерфейс экспертной системы с конечным пользователем?
Уметь: разрабатывать систему проактивной информационной безопасности на основе анализа событий в информационной системе	1.1.Что такое Data Mining?

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: не зачтено
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

КМ-2. Контрольное задание № 3. Практическое задание по использованию статистического метода обработки данных большого объема BigDate. 4. Контрольное задание № 4. Разработка систем проактивной информационной без-опасности на основе анализа событий в информационной системе.

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Контрольное мероприятие проводится в письменной форме

Краткое содержание задания:
Разработка систем проактивной информационной безопасности на основе анализа событий в информационной системе.
Используя материалы, опубликованные в сети Интернет, а также рекомендованную учебную литературу ответить на вопросы.

Контрольные вопросы/задания:

Знать: статистические методы обработки данных большого объема	1.3. Приведите примеры задач, эффективно решаемых методами обработки Big Data
Уметь: использовать технологию Data Mining и оболочки экспертных систем на практике	1.2. Приведите конкретный пример обработки информации о событиях безопасности в информационной системе с применением MapReduce.
Уметь: применять методы и технологии применения ИТ экспертных систем в профессиональной деятельности	1.1.Приложение MapReduce, его назначение, возможности и основы работы

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: не зачтено
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

КМ-3. Контрольное задание № 5. Практическое задание по использованию технологии Data Mining

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Контрольное мероприятие проводится в письменной форме

Краткое содержание задания:
Практическое применение статистических методов Data mining: предварительный ана-лиз природы статистических данных (проверка гипотез стационарности, нормальности, не-зависимости, однородности, оценка вида функции распределения, ее параметров и т.п.); вы-явление связей и закономерностей (линейный и нелинейный регрессионный

анализ, корре-ляционный анализ и др.); многомерный статистический анализ (линейный и нелинейный дискриминантный анализ, кластерный анализ, компонентный анализ, факторный анализ и др.);
динамические модели и прогноз на основе временных рядов.
Практическое применение всех группы методов Data Mining:
- дескриптивный анализ и описание исходных данных;
- анализ связей (корреляционный и регрессионный анализ, факторный анализ, диспер-ионный анализ);
- многомерный статистический анализ (компонентный анализ, дискриминантный анализ, многомерный регрессионный анализ, канонические корреляции и др.);
- анализ временных рядов (динамические модели и прогнозирование).

Контрольные вопросы/задания:

Знать: принципы, методы, технологии и средства извлечения знаний методами Data Mining с использованием деревьев решений	1.1. Что такое реактивная и проактивная концепции в защите информации?

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: не зачтено
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

КМ-4. Контрольное задание № 6. Методы и технологии применения ИТ экспертных систем в про-фессиональной деятельности

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Контрольное мероприятие проводится в письменной форме

Краткое содержание задания:
Методы и технологии применения ИТ экспертных систем в профессиональной деятельности
Используя материалы, опубликованные в сети Интернет, а также рекомендованную учебную литературу ответить на следующие вопросы.

Контрольные вопросы/задания:

Уметь: разрабатывать систему проактивной информационной безопасности на основе анализа событий в информационной системе	1.1. Порядок представления знаний в экспертной системе;

Описание шкалы оценивания:

Оценка: зачтено

Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: не зачтено

Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1 семестр

Форма промежуточной аттестации: Зачет

Процедура проведения

Зачет проводится в устной форме по билетам согласно программе зачета

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ПК-1.5$_{ПК-1}$ Проводит инструментальный мониторинг защищенности компьютерных систем и сетей

Вопросы, задания

1.1.Какова структура экспертных систем?
2.2. В чем заключается интерфейс экспертной системы с конечным пользователем?
3.3.Каков порядок представления знаний в экспертной системе?
4.4.Перечислите и раскройте сущность уровни представления и уровней детальности знаний в экспертной системе?
5.5.Каковы методы поиска решений в экспертных системах?
6.6. Перечислите средства представления знаний и стратегии управления
7.7. Приведите классификацию задач, для решения которых целесообразно использовать экспертные системы.
8.8. Перечислите и дайте общую характеристику основным типам закономерностей в Data Mining
9.9. Перечислите и дайте общую характеристику основным классам систем Data Mining: предметно-ориентированные аналитические системы; статистические пакеты; нейронные сети; деревья решений (decision trees); генетические алгоритмы; алгоритмы ограниченного перебора; системы визуализации многомерных данных
10.10.Опишите порядок извлечения знаний с использованием метода деревьев решений на конкретном примере, связанном с управлением информационными рисками
11.11.Приложение MapReduce, его назначение, возможности и основы работы
12.12.Приведите конкретный пример обработки информации о событиях безопасности в информационной системе с применением MapReduce
13.13. Проактивность и пропускная способность системы. Какова взаимозависимость?
14.14. Проактивная защита и управление информационной безопасностью. В чем основные проблемы?
15.15.Приведите примеры сред разработки экспертных систем.
16.16.Экспертные системы и их практическое применение в приложениях, обеспечивающих информационную безопасность.

Материалы для проверки остаточных знаний

1.1. Что такое экспертная система?

Верный ответ: Экспертная система - компьютерная система, способная частично заменить специалиста-эксперта в разрешении проблемной ситуации. Современные экспертные системы начали разрабатываться исследователями искусственного интеллекта в 1970-х годах, а в 1980-х годах получили коммерческое подкрепление. Предшественники экспертных систем были предложены в 1832 году С. Н. Корсаковым, создавшим механические устройства, так называемые «интеллектуальные машины», позволявшие находить решения по заданным

условиям, например, определять наиболее подходящие лекарства по наблюдаемым у пациента симптомам заболевания

2.2. Что такое Data Mining?
Верный ответ: Data Mining - совокупности методов обнаружения в данных ранее неизвестных, нетривиальных, практически полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности

3.3. Что такое Big Data?
Верный ответ: Big Data - это структурированные или неструктурированные массивы данных большого объема. Их обрабатывают при помощи специальных автоматизированных инструментов, чтобы использовать для статистики, анализа, прогнозов и принятия решений.

4.4. Что такое реактивная и проактивная концепции в защите информации?
Верный ответ: Проактивные стратегии предназначены для прогнозирования вызовов, угроз и возможностей.Проактивный подход ориентирован на планирование на будущее. Кроме того, это помогает распознать и предотвратить потенциальные опасности, прежде чем они появятся. Таким образом, он может предсказать будущее и достичь лучших результатов. Более того, проактивные стратегии часто будут смотреть на организацию с более аналитической точки зрения. Таким образом, они учитывают множество факторов несчастных случаев, жалоб клиентов, претензий, высокой текучести кадров и ненужных расходов. Реактивная стратегия относится к решению проблем после их возникновения, без планирования на долгосрочную перспективу. В некоторых случаях могут возникнуть непредвиденные проблемы, как внутренние, так и внешние. В таких случаях компания должна быстро реагировать.

5.5. В чем сущность сигнатурного метода защиты?
Верный ответ: Методы и принципы защиты теоретически не имеют особого значения, главное чтобы они были направлены на борьбу с вредоносными программами. Но на практике дело обстоит несколько иначе: практически любая антивирусная программа объединяет в разных пропорциях все технологии и методы защиты от вирусов, созданные к сегодняшнему дню. Из всех методов антивирусной защиты можно выделить две основные группы: Сигнатурные методы - точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов.

II. Описание шкалы оценивания

Оценка: зачтено
Описание характеристики выполнения знания: Работа выполнена верно или с несущественными недостатками

Оценка: не зачтено
Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

III. Правила выставления итоговой оценки по курсу