МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»

Кафедра «Вычислительная и прикладная математика»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ
«Защита информации»

Направление подготовки
09.03.04 «Программная инженерия»

Направленность (профиль) подготовки
«Программное обеспечение систем искусственного интеллекта»

Уровень подготовки – бакалавриат

Квалификация выпускника – бакалавр

Форма обучения – очная

Срок обучения – 4 года

Рязань 2023 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы – это совокупность учебно-методических материалов и процедур, предназначенных для оценки качества освоения обучающимися данной дисциплины как части основной образовательной программы.

Цель – оценить соответствие знаний, умений и уровня приобретенных компетенций, обучающихся целям и требованиям основной образовательной программы в ходе проведения текущего контроля и промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности компетенций и индикаторов их достижения, приобретаемых обучающимся в соответствии с этими требованиями.

Контроль знаний обучающихся проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль успеваемости и промежуточная аттестация проводятся с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся, организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков обучающихся на практических занятиях по результатам выполнения и защиты обучающимися индивидуальных заданий, по результатам выполнения контрольных работ и тестов, по результатам проверки качества конспектов лекций и иных материалов.

В качестве оценочных средств на протяжении семестра используется устные и письменные ответы студентов на индивидуальные вопросы, письменное тестирование по теоретическим разделам курса, реферат. Дополнительным средством оценки знаний и умений студентов является отчет о выполнении практических заданий и его защита.

По итогам курса обучающиеся сдают экзамен. Форма проведения – устный ответ с письменным подкреплением по утвержденным билетам, сформулированным с учетом содержания дисциплины. В билет для экзамена включается два теоретических вопроса и задача. В процессе подготовки к устному ответу студент должен составить в письменном виде план ответа.

2. Перечень компетенций с указанием этапов их формирования

При освоении дисциплины формируются следующие компетенцииПК-2 (индикаторы ПК-2.1), ПК-3 (индикаторы ПК-3.3).

Указанные компетенции формируются в соответствии со следующими этапами:

– формирование и развитие теоретических знаний, предусмотренных указанными компетенциями (лекционные занятия, самостоятельная работа студентов);

– приобретение и развитие практических умений предусмотренных компетенциями (практические занятия, самостоятельная работа студентов);

– закрепление теоретических знаний, умений и практических навыков, предусмотренных компетенциями, в ходе решения конкретных задач на занятиях, выполнения индивидуальных заданий на практических занятиях и их защиты, а так же в процессе сдачи экзамена.

3. Показатели и критерии оценивания компетенций (*результатов*) на различных этапах их формирования, описание шкал оценивания

Сформированность каждой компетенции в рамках освоения данной дисциплины оценивается по трехуровневой шкале:

– пороговый уровень является обязательным для всех обучающихся по завершении освоения дисциплины;

– продвинутый уровень характеризуется превышением минимальных характеристик сформированности компетенций по завершении освоения дисциплины;

– эталонный уровень характеризуется максимально возможной выраженностью компетенций и является важным качественным ориентиром для самосовершенствования.

При достаточном качестве освоения более 80% приведенных знаний, умений и навыков преподаватель оценивает освоение данной компетенции в рамках настоящей дисциплины на эталонном уровне, при освоении более 60% приведенных знаний, умений и навыков – на продвинутом, при освоении более 40% приведенных знаний умений и навыков – на пороговом уровне. При освоении менее 40% приведенных знаний, умений и навыков компетенция в рамках настоящей дисциплины считается неосвоенной.

Уровень сформированности каждой компетенции на различных этапах ее формирования в процессе освоения данной дисциплины оценивается в ходе текущего контроля успеваемости и представлено различными видами оценочных средств.

Оценке сформированности в рамках данной дисциплины подлежат компетенции/индикаторы:

Показатели достижения планируемых результатов обучения и критерии их оценивания на разных уровнях формирования компетенций приведены в таблице 1.

Таблица 1. Показатели достижения индикаторов компетенции

1	2	3	4
Компетенция: код по ФГОС 3++, формулировка	**Индикаторы**	**Этап**	**Наименование оценочного средства**
ПК-2 (09.03.04/02 Программно-алгоритмическое обеспечение систем искусственного интеллекта) Способен классифицировать и идентифицировать задачи искусственного интеллекта, выбирать адекватные методы и инструментальные средства решения задач искусственного интеллекта	**ПК-2.1 Классифицирует и идентифицирует задачи систем искусственного интеллекта в зависимости от особенностей проблемной и предметной областей** ЗНАТЬ - основные определения искусственного интеллекта и систем искусственного интеллекта, историю развития науки об искусственном интеллекте, эволюцию и главные тренды систем ИИ; классы решаемых задач с помощью СИИ; основные параметры идентификации задач ИИ; назначение, сфера применения, виды используемых знаний, временные аспекты решения задач УМЕТЬ - определять принадлежность проблемной и предметной областей	1	Зачет

1	2	3	4
	к классу решаемых задач с помощью систем ИИ и основные параметры идентификации задач СИИ ВЛАДЕТЬ - особенностями классификации и идентификации задач искусственного интеллекта для различных предметных областей.		
ПК-3 (09.03.04/02 Программно-алгоритмическое обеспечение систем искусственного интеллекта) Способен разрабатывать и тестировать программные компоненты решения задач в системах ИИ	**ПК-3.3 Проводит тестирование систем искусственного интеллекта** Знать: основные критерии качества систем искусственного интеллекта, методы и инструментальные средства тестирования работоспособности и качества функционирования систем искусственного интеллекта. Уметь: проводить тестирование работоспособности и качества функционирования систем искусственного интеллекта и проверять выполнение требований к системам искусственного интеллекта со стороны пользователя. Владеть: методологией тестирования систем искусственного интеллекта.		

Преподавателем оценивается содержательная сторона и качество материалов, приведенных в отчетах студента по практическим занятиям. Кроме того, преподавателем учитываются ответы студента на вопросы по соответствующим видам занятий при текущем контроле:

– контрольные опросы;

– задания для практических занятий.

Принимается во внимание **знания** обучающимися:

- теоретических основ защиты информации;
- алгоритмов защиты информации и их практическая реализация;
- защиты программ от нелегального копирования;
- методов и алгоритмов сжатия данных.

умений:

- применять методы проектирования программного обеспечения и его программную реализацию;
- осуществлять сбор и обобщение информации о проблемной области путем опроса

экспертов, исходных данных о функционировании проблемной области, документированных источников знаний, а также формировать требования к системе искусственного интеллекта.

обладание навыками**:**

- реализации электронного аналога шифровальной машины «Энигма»;
- реализации алгоритма шифрования с открытым ключом (RSA);
- реализации алгоритма симметричного шифрования (AES);
- реализации алгоритма симметричного шифрования (DES)

Критерии оценивания уровня сформированности компетенции в процессе выполнения практических работ:

41%-60% правильных ответов соответствует пороговому уровню сформированности компетенции на данном этапе ее формирования;

61%-80% правильных ответов соответствует продвинутому уровню сформированности компетенции на данном этапе ее формирования;

81%-100% правильных ответов соответствует эталонному уровню сформированности компетенции на данном этапе ее формирования.

Сформированность уровня компетенций не ниже порогового является основанием для допуска обучающегося к промежуточной аттестации по данной дисциплине.

Формой промежуточной аттестации по данной дисциплине является зачет, оцениваемый по принятой в ФГБОУ ВО «РГРТУ» системе: «зачтено» и «не зачтено».

Критерии оценивания промежуточной аттестации представлены в таблице.

Шкала оценивания	Критерии оценивания
«зачтено»	**оценки «зачтено»** заслуживает обучающийся, продемонстрировавший полное знание материала изученной дисциплины, усвоивший основную литературу, рекомендованную рабочей программой дисциплины; выполнивший все практические задания; показавший систематический характер знаний по дисциплине, ответивший на все вопросы билета или допустивший погрешность в ответе вопросы, но обладающий необходимыми знаниями для их устранения под руководством преподавателя;
«не зачтено»	**оценки «не зачтено»** заслуживает обучающийся, не выполнивший практические задания, продемонстрировавший серьезные пробелы в знаниях основного материала изученной дисциплины, не ответивший на все вопросы билета и дополнительные вопросы. Оценка «не зачтено» ставится обучающимся, которые не могут продолжить обучение по образовательной программе без дополнительных занятий по соответствующей дисциплине (формирования и развития компетенций, закрепленных за данной дисциплиной).

4. Типовые контрольные задания или иные материалы

ФОС по дисциплине содержит следующие оценочные средства, позволяющие оценить знания, умения и уровень приобретенных компетенций при текущем контроле и промежуточной аттестации, разбитые по модулям дисциплины:

- перечни экзаменационных вопросов;
- макеты билетов к экзамену.

Средства для оценки различных уровней формирования компетенций по категориям «знать», «уметь», «владеть» обеспечивают реализацию основных принципов контроля, таких, как объективность и независимость, практико-ориентированность, междисциплинарность.

С учетом этого, контрольные вопросы (задания, задачи,) входящие в ФОС, для различных категорий и уровней освоения компетенций имеют следующий вид:

Уровень ЗНАТЬ

Дескрипторы	Пример задания из оценочного средства
основные определения искусственного интеллекта и систем искусственного интеллекта, историю развития науки об искусственном интеллекте, эволюцию и главные тренды систем ИИ; классы решаемых задач с помощью СИИ; основные параметры идентификации задач ИИ; назначение, сфера применения, виды используемых знаний, временные аспекты решения задач	1. Дать определения следующих терминов: информация, защита информации, актив, информационная сфера, угроза, безопасность, информационная безопасность. 2. Перечислить модели доступа и описать особенности каждой из них. 3. Привести виды случайных чисел, и дать примеры алгоритмов их вычисления. Зачем нужны случайные числа.

Уровень УМЕТЬ

Дескрипторы	Пример задания из оценочного средства
определять принадлежность проблемной и предметной областей к классу решаемых задач с помощью систем ИИ и основные параметры идентификации задач СИИ	1. Дать определения следующих терминов: идентификация, авторизация, аутентификация. Дать примеры каждого из них. 2. Дать определение следующих терминов: шифрование, рассеивание. Требования к алгоритмам шифрования. Привести правила Керкхоффа.
проводить тестирование работоспособности и качества функционирования систем ИИ и проверять выполнение требований к системам ИИ со стороны пользователя	3. Привести алгоритм линейного конгруэнтного генератора. Какое распределение он дает? Какое распределение можно из него получить и с помощью какого преобразования?

Перечни вопросов к зачету

7 семестр

1. Какова цель моделирования угроз. Перечислить этапы моделирования угроз. Перечислить уровни возможности нарушителей. Дать определения термина угроза. Перечислить виды источников угроз.

2. Виды симметричного шифрования (поточные и блочные). Привести схему для одного из видов.

3. Какое шифрование называется симметричным? Описать алгоритм шифрования DES или AES.

4. Привести классификацию автоматизированных систем с точки зрения требований безопасности (3 класса защищенности). Перечислить подсистемы защиты

информации в автоматизированных системах.

5. Дать определения алгоритмов перестановки и подстановки. Привести примеры каждого из этих видов алгоритмов. Привести пример алгоритма, использующего оба подхода.

6. Дать определение асимметричного шифрования. Описать алгоритм шифрования RSA. Кто создает ключи: отправитель или получатель?

7. Дать определение одно- и многоалфавитных подстановок. К какому виду относится алгоритм Энигма. Привести схему алгоритма Энигма.

8. Описать алгоритм создания цифровой подписи. Описать алгоритм проверки цифровой подписи.

9. Дать определение электронной цифровой подписи. Дать определение электронного сертификата. Какие существуют модели организации инфраструктуры электронных сертификатов?

Перечень лабораторных работ

ЛР1.1 - ЛР1.2 Реализация электронного аналога шифровальной машины «Энигма».
Цель работы:
Разработка электронного аналога шифровальной машины.
Задание:

Реализовать в виде программы электронный аналог шифровальной машины «Энигма». Обеспечить шифрование и расшифровку произвольного файла с использованием разработанной программы. Предусмотреть работу программы с пустым, однобайтовым файлом. Программа также должна уметь обрабатывать файл архива (rar, zip или др.).

ЛР1.3 - ЛР2.1 Реализация алгоритма шифрования с открытым ключом (RSA).
Цель работы:
Разработка алгоритма шифрования с открытым ключом.
Задание:

Реализовать программу шифрования алгоритмом с открытым ключом. Использовать алгоритм RSA. Обеспечить шифрование и расшифровку произвольного файла с использованием разработанной программы. Предусмотреть работу программы с пустым, однобайтовым файлом. Программа также должна уметь обрабатывать файл архива (rar, zip или др.).

ЛР2.2 - ЛР2.3 Реализация алгоритма симметричного шифрования (DES).
Цель работы:
Разработка алгоритма симметричного шифрования (DES).
Задание:

Реализовать программу шифрования симметричным алгоритмом DES.Обеспечить шифрование и расшифровку произвольного файла с использованием разработанной программы. Предусмотреть работу программы с пустым, однобайтовым файлом. Программа также должна уметь обрабатывать файл архива (rar, zip или др.).

ЛР2.4 - ЛР3.1 Реализация алгоритма симметричного шифрования (AES).
Цель работы:
Разработка алгоритма симметричного шифрования (AES).
Задание:

Реализовать программу шифрования алгоритмом с открытым ключом. Использовать алгоритм RSA. Обеспечить шифрование и расшифровку произвольного файла с ис-

пользованием разработанной программы. Предусмотреть работу программы с пустым, однобайтовым файлом. Программа также должна уметь обрабатывать файл архива (rar, zipили др.).

ЛР3.2 - ЛР3.3 Создание и проверка электронной подписи для документа.
Цель работы:
Создание электронной подписи.
Задание:

Реализовать программу создания и проверки электронной подписи для документа. Обеспечить шифрование и расшифровку произвольного файла с использованием разработанной программы. Предусмотреть работу программы с пустым, однобайтовым файлом. Программа также должна уметь обрабатывать файл архива (rar, zip или др.).