Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Механико-математический факультет

УТВЕРЖДЕНО:
Декан ММФ ТГУ
Л.В.Гензе

Оценочные материалы по дисциплине

Основы криптографии

по направлению подготовки

01.03.01 Математика
02.03.01 Математика и компьютерные науки

Направленность (профиль) подготовки
Основы научно-исследовательской деятельности в области математики
Основы научно-исследовательской деятельности в области математики и компьютерных наук

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2023

СОГЛАСОВАНО:
Руководитель ОП
Л.В.Гензе

Председатель УМК
Е.А.Тарасов

Томск – 2023

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-4 Способен проводить под научным руководством исследование на основе существующих методов в конкретной области профессиональной деятельности.

ПК-1 Способен проводить научно-исследовательские разработки по отдельным разделам выбранной темы.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК 4.1 Проводит поиск и обработку научной и научно-технической информации, необходимой для решения исследовательских задач

ИОПК 4.2 Оценивает полученные результаты и формулирует выводы по итогам проведенных исследований

ИПК 1.1 Проводит работы по обработке и анализу научно-технической информации и результатов исследований

ИПК 1.2 Подготавливает планы и программы проведения отдельных этапов научно-исследовательской работы

ИПК 1.3 Проводит отдельные этапы научно-исследовательской работы

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– тесты;

Тест (ИОПК-4.2, ИОПК-4.1)

1. Вам дан шифр-текст «пгхзпгхлнг» и вы знаете, что был использован шифр Цезаря. Расшифруйте сообщение и определите сдвиг алфавита:
   а) сдвиг на 3 влево
   б) сдвиг на 7 вправо
   в) сдвиг на 4 влево
   г) сдвиг на 3 вправо
2. Какая из нижеперечисленных криптосистем не является симметричной:
   а) RSA
   б) AES
   в) DES
   г) Шифр Ривеста

Ключи: 1 г), 2 а).

Критерии оценивания: тест считается пройденным, если обучающий ответил правильно как минимум на половину вопросов.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Зачет проводится устно. Билет состоит из 2-х вопросов, проверяющих ИОПК 4.1, ИОПК-4.2. Ответы на вопросы даются в развернутой форме и могут предполагать решение задач и краткую интерпретацию полученных результатов.

На подготовку билета отводится 90 мин.

Примеры теоретических вопросов:

1. Протокол RSA.

2. Вероятностный шифр Эль-Гамаля.
3. Многоалфавитные шифры замены.
4. Итеративные блочные шифры. Шифры Фейстеля.
5. Система Диффи-Хэллмана.
6. Формальные модели шифров.
7. Совершенные шифры.

Критерии оценивания:

Результаты зачета определяются оценками «зачтено» и «не зачтено». При ответе на вопрос оценивается полнота и точность ответа, логичность и аргументированность изложения материала, умения использовать в ответе фактический материал.

Зачет выставляется, если даны правильные ответы на все вопросы билета, либо даны полные ответы, но имеются некритичные логические несоответствия, при этом форма изложения достаточно ясная и понятная, либо данные ответы не являются полными, но изложенная часть логически не противоречива и изложена ясно и понятно.

Зачет не выставляется, если ответ является неполным, изложение логически противоречиво, но понятно, либо дан неполный логически противоречивый недоказательный ответ, либо ответ отсутствует по сути.

Студент имеет право проходить промежуточную аттестацию вне зависимости от результатов текущей успеваемости.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Тест

1. Что в переводе с греческого языка означает слово «криптография»? (ИОПК-4.1.)
   а) цифра
   б) распознание
   в) преобразование
   г) тайнопись
2. Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства? (ИОПК-4.1.)
   а) Шифр Цезаря
   б) Шифр Бэбиджа
   в) Шифр Энигма
   г) Шифр Виженера

Ключи: 1 г), 2 а).

Информация о разработчиках

Норбосамбуев Цырендоржи Дашацыренович, к.ф.-м.н., доцент кафедры алгебры ММФ ТГУ