МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Тульский государственный университет»

Институт прикладной математики и компьютерных наук
Кафедра «Прикладная математика и информатика»

Утверждено на заседании кафедры
«Прикладная математика и информатика»
24 января 2022 г., протокол № 5

Заведующий кафедрой
_____М.В. Грязев

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ОЦЕНОЧНЫЕ МАТЕРИАЛЫ) ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

«Методы защиты информации»

основной профессиональной образовательной программы высшего образования – программы бакалавриата

по направлению подготовки
01.03.02 Прикладная математика и информатика

с направленностью (профилем)
Прикладная математика и информатика

Форма обучения: очная

Идентификационный номер образовательной программы: 010302-01-22

Тула 2022 год

ЛИСТ СОГЛАСОВАНИЯ
фонда оценочных средств (оценочных материалов)

Разработчик:

Горбачев Дмитрий Викторович, профессор, д.ф.-м.н. _____
(ФИО, должность, ученая степень, ученое звание) *(подпись)*

1. Описание фонда оценочных средств (оценочных материалов)

Фонд оценочных средств (оценочные материалы) включает в себя контрольные задания и (или) вопросы, которые могут быть предложены обучающемуся в рамках текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю). Указанные контрольные задания и (или) вопросы позволяют оценить достижение обучающимся планируемых результатов обучения по дисциплине (модулю), установленных в соответствующей рабочей программе дисциплины (модуля), а также сформированность компетенций, установленных в соответствующей общей характеристике основной профессиональной образовательной программы.

Полные наименования компетенций и индикаторов их достижения представлены в общей характеристике основной профессиональной образовательной программы.

2. Оценочные средства (оценочные материалы) для проведения текущего контроля успеваемости обучающихся по дисциплине (модулю)

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ПК-2 (контролируемый индикатор достижения компетенции ПК-2.1)

1. Проблемы защиты информации
2. Защита от потерь
3. Защита от несанкционированного доступа
4. Стандарты информационной безопасности
5. Приложения к базам данных и Web

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ПК-4 (контролируемый индикатор достижения компетенции ПК-4.1)

1. Работа с нечетко заданной информацией
2. Регулярные выражения, поиск и замена текста
3. Синтаксис PERL-совместимых регулярных выражений. Примеры
4. Сжатие информации при помощи префиксных кодов
5. Двоичная арифметика, префиксные коды

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ПК-2 (контролируемый индикатор достижения компетенции ПК-2.2)

1. Код Шэнона–Фэно, пример
2. Код Хаффмана, пример
3. Словарные методы сжатия. Общие сведения
4. Алгоритм Лемпеля–Зива (LZ)
5. Алгоритм Лемпеля–Зива–Велча (LZW)

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ПК-4 (контролируемый индикатор достижения компетенции ПК-4.2)

1. Алгоритм сжатия BZIP. Преобразование Барроуза–Уиллера. Описание алгоритма. Пример
2. Поле вычетов по простому модулю
3. Кольцо вычетов, быстрое вычисление остатка
4. Расширенный алгоритм Евклида
5. Малая теорема Ферма, теорема Эйлера

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ПК-2 (контролируемый индикатор достижения компетенции ПК-2.3)

1. Поле вычетов
2. Поле Галуа
3. Кольцо многочленов над полем вычетом. Пример поля из 8 элементов
4. Конструкция поля Галуа, дискретный логарифм
5. Для фразы: ДОЛОТОДОЛОТОДОЛОТОДОЛОТО: построить код Хаффмана, применить алгоритм LZ77, применить алгоритм LZW

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ПК-4 (контролируемый индикатор достижения компетенции ПК-4.3)

1. Раскодировать фразу, закодированную LZW (сколько слов?): 3,1,2,1,4,6,8,10,3 (словарь: О – 1, Л – 2, Б – 3, Т – 4)Контрольные суммы. Назначение контрольных сумм
2. Хеш-функции
3. CRC-код
4. Коды, исправляющие ошибки. Постановка задачи, код Хемминга
5. Необходимые утверждения, линейные коды

3. Оценочные средства (оценочные материалы) для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ПК-2 (контролируемый индикатор достижения компетенции ПК-2.1)

1. БЧХ-коды
2. Введение в криптографию. Терминология, исторические примеры шифрования
3. Симметричные и ассиметричные шифры
4. Криптоанализ
5. Симметрические криптоалгоритмы. Введение, шифр Вернама, оценка стойкости шифра
6. Назначение Firewall
7. Что такое Telnet порт
8. Способы блокировки сетевых программ
9. Как можно узнать открытые порты
10. Назначение виртуальной машины

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ПК-4 (контролируемый индикатор достижения компетенции ПК-4.1)

1. Нарушение условий стойкости, примеры атак на шифр
2. Блочные шифры, условия стойкости, примеры
3. Сеть Фейштеля, шифр TEA
4. По схеме Хемминга принята кодовая последовательность: 1010010. Какая 16-я цифра была послана?
5. Чему равно CRC3(2Ah)

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ПК-2 (контролируемый индикатор достижения компетенции ПК-2.2)

1. Криптографические хэш-функции. Введение, свойства криптографических хеш-функций
2. Использование блочных шифров для построения хэш-функций
3. Примеры криптографических хэш-функций
4. Приложения хэш-функций, генерация ключей, аутентификация

5. Криптоанализ хэш-функций, радужные таблицы, использование «соли»
6. Пример программы для синхронизации данных
7. Назначение контрольной суммы
8. Назначение регулярного выражения
9. Разница между UTF8 и ASCII
10. Пример программы восстановления файлов

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ПК-4 (контролируемый индикатор достижения компетенции ПК-4.2)

1. Асимметричные криптоалгоритмы с открытым ключом, основные сведения. Односторонние функции
2. Алгоритм Диффи–Хеллмана. Практическое применение
3. Алгоритм RSA. Исторический экскурс. Описание алгоритма RSA, пример. Практическое применение
4. Криптографические протоколы, основные сведения
5. Основные криптопротоколы, цифровая подпись.

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ПК-2 (контролируемый индикатор достижения компетенции ПК-2.3)

1. Сетевые команды
2. Создание Telnet соединения
3. Управление удаленным компьютером по Telnet
4. Брандмауэр Windows
5. Мониторинг сети
6. Виртуальная машина
7. Приемы работы с данными
8. Восстановление удаленных файлов
9. Восстановление данных на физическом уровне
10. Надежная очистка

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенции ПК-4 (контролируемый индикатор достижения компетенции ПК-4.3)

1. Шифрование при помощи архиватора
2. Проблемы шифрования при помощи архиватора
3. Прозрачное шифрование в Windows
4. Сертификат шифрования Windows
5. Назначение команды: echo, cd, dir, copy, echo pause>>test.cmd, shutdown, ipconfig, hostname, ping, tracert