|  |  |
| --- | --- |
| Приложение 4 к рабочей программе дисциплины | |
| ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ | |
| Фонд оценочных средств | |
| Направление/ специальность подготовки | 11.04.01 Радиотехника |
| Специализация/ профиль/ программа подготовки | Системы и устройства передачи, приема и обработки сигналов |
| Уровень высшего образования | Магистратура |
| Форма обучения | Очная, заочная |
| Факультет | И Информационные и управляющие системы |
| Выпускающая кафедра | И4 Радиоэлектронные системы управления |
| Кафедра-разработчик | И4 Радиоэлектронные системы управления |
| Год приема | 2023 |

**ФОС по дисциплине «ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ»**

**ОП ВО 11.04.01 Радиотехника «Системы и устройства передачи, приема и обработки сигналов», формы обучения очная, заочная**

ПСК-1.1 - способен самостоятельно осуществлять постановку задачи исследования, формирование плана его реализации, выбор методов исследования и обработку результатов;\

ПСК-1.3 - способен разрабатывать и обеспечивать программную реализацию эффективных алгоритмов решения сформулированных задач с использованием современных языков программирования

|  |  |  |  |
| --- | --- | --- | --- |
| **Номер задания** | **Содержание вопроса** | **Компетенция** | **Время ответа, мин.** |
|  | Определить количество информации геометрической мерой информационного сообщения 9 бит:  81  11  38742  512 | ПСК-1.1 | 3 |
|  | Определить количество информации в комбинаторной мере для двоичной системы счисления при условии, что передается два сообщения величиной 9 бит и 5 бит  16384  16  59050  544 | ПСК-1.1 | 3 |
|  | Энтропия равна 0, когда вероятность наступления события pi=  0  1  0.5  1/е | ПСК-1.1 | 1 |
|  | Для осуществления какого эффекта требуется поперечное магнитное поле?  Фотогальванический  Пироэлектрический  Зеебека  Холла | ПСК-1.1 | 1 |
|  | Определить максимальную скорость (бит/с) передачи информации двоичными сигналами в бесшумном канале, если полоса пропускания равна 542кГц  542  542000  293764  1084  1084000 | ПСК-1.1 | 5 |
|  | Определить максимальную скорость передачи двоичных данных в реальном канале, если полоса пропускания канала 19 Гц, отношение сигнал/шум 57 Дб | ПСК-1.1 | 10 |
|  | Одномодовые или многомодовые - это параметр:  акустической линии связи витой пары  радиоволн  оптоволокна | ПСК-1.1 | 1 |
|  | Волны, которые могут проникать под воду на ограниченное расстояние, относятся к:  Средним  Длинным  Коротким  Сверхдлинным | ПСК-1.1 | 1 |
|  | Определить нижнюю границу частот в передаваемом сообщении, если пропускная способность канала составляет 970414 бит/с. Ответ представить в Гц NRZ | ПСК-1.1 | 5 |
|  | Определить кодовое расстояние по Хеммингу двух кодовых комбинаций: 111000111 и 101010111 | ПСК-1.1 | 2 |
|  | Определить вероятность пропуска ошибки при передаче четырех информационных разрядов кода с контролем четности, если вероятность безошибочной передачи равна 0,96.  !!!Учесть суммарное количество разрядов кода! | ПСК-1.1 | 8 |
|  | Определить вес кодовой комбинации: 110011001111100 | ПСК-1.1 | 1 |
|  | Вычислить коэффициент сжатия, если длина исходного сообщения  равна 818, длина сжатого - 700 | ПСК-1.1 | 4 |
|  | Минимальное количество ключей, необходимое для приватного общения группы из 40 пользователей равно | ПСК-1.1 | 5 |
|  | Зашифровать с помощью афинного шифра (2,1) букву А русского алфавита (позиции алфавита 0:32) | ПСК-1.1 | 7 |
|  | ADFGVX является шифром:  перестановочным  подстановочным  подстановочно-перестановочным  гаммирования | ПСК-1.1 | 1 |
|  | Определить значение функции Эйлера для числа 33 | ПСК-1.1 | 5 |
|  | Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:  2  1  4  2^n | ПСК-1.1 | 1 |
|  | Как связаны ключи друг с другом в системе с открытым ключом:  экзистенциально  логически  алгоритмически  математически | ПСК-1.1 | 1 |
|  | На алгоритме Люцифер базируется:  AES  DES  RSA  Диффи-Хеллмана | ПСК-1.1 | 1 |
|  | Определить количество информации в комбинаторной мере для двоичной системы счисления при условии, что передается два сообщения величиной 2 бит и 7 бит  512  132  9  128 | ПСК-1.3 | 3 |
|  | Сообщения передаются 6-разрядным и 8-разрядным двоичным кодом. Определить количество информации статистической мерой при передаче двух сообщений разрядности 6 и 8, при условии равенства вероятности появления всех элементов алфавита  320  14  8  256 | ПСК-1.3 | 3 |
|  | Энтропия равна 0, когда вероятность наступления события pi=  0  1  0.5  1/е | ПСК-1.3 | 1 |
|  | Энтропия максимальна, когда вероятность наступления события pi=  1  0  0.5  1/i | ПСК-1.3 | 1 |
|  | Определить максимальную скорость (бит/с) передачи информации двоичными сигналами в бесшумном канале, если полоса пропускания равна 542кГц  542  542000  293764  1084  1084000 | ПСК-1.3 | 5 |
|  | Определить максимальную скорость передачи двоичных данных в реальном канале, если полоса пропускания канала 346 Гц, отношение сигнал/шум 24 Дб | ПСК-1.3 | 10 |
|  | Определить ширину спектра в передаваемом сообщении, если пропускная способность канала составляет 812703 бит/с. Ответ представить в Гц | ПСК-1.3 | 8 |
|  | Определить требуемое минимальное расстояние по Хеммингу для обнаружения 11-кратной ошибки | ПСК-1.3 | 3 |
|  | Определить требуемое минимальное расстояние по Хеммингу для обнаружения 12-кратной ошибки и исправления 7-кратной | ПСК-1.3 | 3 |
|  | Избыточность кода с 112 информационными  и 13 проверочными битами равна | ПСК-1.3 | 4 |
|  | Вычислить разрешенную кодовую комбинацию циклического кода для информационной последовательности 1001 и образующего полинома 1011 | ПСК-1.3 | 8 |
|  | Вычислить степень сжатия, если длина исходного сообщения  равна 888, длина сжатого - 542 | ПСК-1.3 | 4 |
|  | Является ли следующая последовательность кодов префиксным кодом?  00  10  11  010  011 | ПСК-1.3 | 5 |
|  | Алгоритмом шифрования называют:  Ключ шифрования Кодирование  Правило шифрования  Пара правило-ключ | ПСК-1.3 | 1 |
|  | Если буквы меняют свои позиции, но сохраняют свои роли, то это:  шифр подстановки  шифр Цезаря  шифр Полибия  перестановочное шифрование | ПСК-1.3 | 1 |
|  | ADFGVX является шифром:  перестановочным  подстановочным  подстановочно-перестановочным  гаммирования | ПСК-1.3 | 1 |
|  | Найти пропущенную в номере банковской карты цифру:  4539451203X87356 | ПСК-1.3 | 7 |
|  | К асимметричным методам относятся:  Эллиптических кривых  BB84  RSA  Эль-Гамаля  DES  Диффи-Хеллмана  AES | ПСК-1.3 | 2 |
|  | Количество используемых ключей в системах с открытым ключом:  2  1  4  2^n | ПСК-1.3 | 1 |
|  | Выберите то, что используют для создания цифровой подписи:  Открытый ключ получателя  Открытый ключ отправителя   Закрытый ключ получателя  Закрытый ключ отправителя | ПСК-1.3 | 1 |