

Демонстрационный вариант и методические рекомендации
по направлению «Бизнес-информатика»

Профиль: «Управление информационной безопасностью»

КОД – 172

ДЕМОНСТРАЦИОННЫЙ ВАРИАНТ

Время выполнения задания – 240 мин., язык – русский.

Предварительные критерии оценивания работ участников олимпиадных состязаний
Максимально возможная оценка составляет 100 баллов.

За правильное решение задач общей части суммарно может быть начислено максимум 20 баллов.

За правильный и полный ответ на вопросы, сформулированные в каждом из блоков специальной части, может быть начислено максимум 20 баллов, суммарно, по каждому из блоков. Максимум за ответы по специальной части составляет 80 баллов.

При решении задач особое внимание обращается на применяемую учащимся методику получения ответа, приводимые расчеты, обоснования и логику получения ответа.

При оценке эссе анализируется правильность ответа, понимание и особенности авторской оценки раскрываемой темы.

1. Дайте развернутый ответ.

1.1. Что общего и в чем различия между информационной, компьютерной и автоматизированной системами?

1.2. Защищают ли межсетевые экраны от всех атак на компьютерную систему? Если нет, то, какие еще способы защиты существуют?

2. Решите задачи.

2.1. Представьте число 947 в псевдосистеме счисления, которая описывается следующей формулой:

$$A = a_1 * k_1 + a_2 * k_2 + \dots + a_n * k_n,$$

где a_1, \dots, a_n – цифры искомого числа, k_1, \dots, k_n – разряды числа, равные значениям факториалов чисел ($k_1 = 1, k_2 = 2, k_3 = 6, k_4 = 24, \dots$).

2.2. Музыкальный файл нового формата .mus состоит из набора фреймов длительностью 1 мс. Каждый фрейм состоит из заголовка фрейма длины 10 байт и тела фрейма некоторой постоянной длины. В заголовке фрейма присутствует бит ошибки. Если он равен «1», данный фрейм считается искаженным и плеером не воспроизводится. Количество искаженных фреймов не должно превышать 0,1%. Какой объем информации можно скрыть в файле формата .mus размером 3 МБ и длительностью 3 минуты с использованием искаженных фреймов, чтобы не вызвать при этом подозрений.

2.3. Решение данной задачи связано с использованием различных систем счисления. Для усложнения задачи введены дополнительные условия, требующие от участника олимпиады выполнить ряд предварительных действий, не связанных с применением специальных знаний, а рассчитанных, скорее, на смекалку. В частности, используется оригинальное основание системы счисления.

Сначала определим разряды факториальной псевдосистемы счисления, которыми мы можем воспользоваться для представления искомого числа:

$$k_0 = 1, k_1 = 2, k_2 = 6, k_3 = 24, k_4 = 120, k_5 = 720 \tag{1}$$

Переведем число 947 в новую псевдосистему счисления. Для этого будем делить 947 на разряды из (1) последовательно, начиная с максимального. Целая часть результата станет цифрами искомого числа, остаток от деления будем делить на следующий разряд:

$$947 : 720 = 1. \text{ Остаток } 227.$$

$$227 : 120 = 1. \text{ Остаток } 107.$$

$$107 : 24 = 4. \text{ Остаток } 11.$$

$$11 : 6 = 1. \text{ Остаток } 5.$$

$$5 : 2 = 2. \text{ Остаток } 1.$$

Получим 114121.

Для проверки производим обратные действия:

$$1*1 + 2*2 + 1*6 + 4*24 + 1*120 + 1*720 = 947.$$

Перевод выполнен правильно.

2.4. Данная задача относится к задачам скрытой передачи информации. Однако условие задачи не является сложным для понимания и требует от решающего только самых общих знаний в области обработки компьютерной информации.

Найдем количество фреймов в файле:

$$3 \text{ мин} = 180 \text{ сек} = 180000 \text{ мс}.$$

Количество искаженных фреймов не должно превышать 0,1 %:

$$180\,000 * 0,001 = 180 \text{ фреймов}.$$

Вычислим размер одного фрейма:

$$3 \text{ Мб} = 3 * 1024 \text{ Кб} = 3 * 1024 * 1024 \text{ б}$$

$$3 * 1024 * 1024 / 180000 = 17,47 \text{ байт}.$$

Из соображений работы с целыми числами положим размер одного фрейма 17 байт:

$$17 \text{ байт} = 17 * 8 \text{ бит} = 136 \text{ бит}.$$

Предположим, что информация может быть скрыта как в заголовке, так и в теле фрейма. Тогда из 136 бит можно использовать 135 бит для скрываемого сообщения, так как один бит является показателем того, что данный фрейм является испорченным и его нельзя использовать.

$$135 \text{ бит} * 180 \text{ фреймов} = 24300 \text{ бит}.$$

Таким образом, при заданных условиях в файле можно скрыть до 24300 бит информации.

3. Выберите один правильный ответ среди предложенных и заштрихуйте соответствующий ему овал в бланке ответов на пересечении номера вопроса и номера ответа.

1. Какой из нормативно-правовых документов относится к определяющему концептуальные основы обеспечения информационной безопасности в России?

- 1) кодекс административных правонарушений;
- 2) трудовой кодекс;
- 3) уголовно-процессуальный кодекс;
- 4) Конституция РФ.

Ответ: Конституция РФ.

2. Какое из понятий подходит под данное определение: юридический процесс получения некоторым образом каким-либо субъектом права на осуществление определенного вида деятельности?

- 1) аттестация;
- 2) лицензирование;

3) сертификация;

4) специализация.

Ответ: лицензирование

3. Какое из понятий подходит под данное определение: процесс установления соответствия некоторого товара (услуги) данным требованиям?

1) аттестация;

2) лицензирование;

3) сертификация;

4) специализация.

Ответ: сертификация

4. Что понимают под политикой безопасности в компьютерной системе (КС)?

1) качественно или качественно-количественное выражение свойств допустимости в терминах, представляющих КС;

2) качественно или качественно-количественная мера разрешенных свойств КС;

3) система мер, направленная на защиту информации в системе;

4) набор норм, правил и тактических приемов, которые регулируют управление, защиту и распределенную ценную информацию в системе.

Ответ: набор норм, правил и тактических приемов, которые регулируют управление, защиту и распределенную ценную информацию в системе

5. Что относится к дискреционной политике безопасности?

1) все субъекты и объекты системы не идентифицируются;

2) все права доступа субъекта к объекту системы определяются на основе некоторых внешних правил;

3) все права доступа объекта к субъекту системы определяются на основе некоторых внешних правил;

4) каждому субъекту и объекту соответственно должна быть присвоена определенная метка секретности.

Ответ: все права доступа субъекта к объекту системы определяются на основе некоторых внешних правил

6. Что относится к мандатной политике безопасности?

1) все субъекты и объекты системы не идентифицируются;

2) все права доступа субъекта к объекту системы определяются на основе некоторых внешних правил;

3) все права доступа объекта к субъекту системы определяются на основе некоторых внешних правил;

4) каждому субъекту и объекту соответственно должна быть присвоена определенная метка секретности.

Ответ: каждому субъекту и объекту соответственно должна быть присвоена определенная метка секретности

7. Какое из понятий подходит под данное определение: однонаправленное преобразование исходной информации в комбинацию символов фиксированной длины?

- 1) цифровая подпись;
- 2) хэш-функция;
- 3) кодирование;
- 4) аутентификация.

Ответ: хэш-функция

8. Какое из понятий подходит под данное определение: комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами?

- 1) сетевой адаптер;
- 2) сетевой фильтр;
- 3) сетевой сканер;
- 4) сетевой экран.

Ответ: сетевой экран

4. Прочитайте статью и сделайте ее критический анализ на русском языке.

Watermarking as a Means to Enhance Biometric Systems: A Critical Survey

Jutta Hammerle-Uhl, Karl Raab, and Andreas Uhl

Multimedia Signal Processing and Security Lab (WaveLab)

Department of Computer Sciences, University of Salzburg, Austria

Contact author e-mail: uhl@cosy.sbg.ac.at

Abstract. Watermarking is discussed as possible means to enhance biometric systems. Application scenarios for the employment of watermarks as found in literature are discussed and analysed with respect to required watermark properties, possible attacks, and eventual (cryptographic) alternatives.

5. Выберите одну из предложенных тем и напишите эссе по этой теме:

1. Роль криптографии в защите персональных данных.
2. Применение виртуальных частных сетей в защищенной передаче данных

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

При подготовке к олимпиаде рекомендуется использовать учебники и учебные пособия по следующим отраслям знаний:

1. Теория систем и системного анализа;
2. Криптографические методы защиты информации;
3. Информационное право;
4. Статистические методы;
5. Информационная и компьютерная безопасность;
6. Право интеллектуальной собственности.

Рекомендуется ознакомиться с нормативно-правовой базой Европейской практики регулирования защиты персональных данных.

При подготовке и ответы на олимпиадные задания рекомендуется в первую очередь, определить к какой отрасли знаний относится данный вопрос, далее продемонстрировать методику и логику получения ответа, приводимые расчеты и обоснования.

При написании эссе следует отобразить индивидуальный подход к предлагаемой тематике, в отношении объема и функций, - на грани научной статьи и литературного очерка. При подготовке и написании рекомендуется продемонстрировать образность мышления, подвижность ассоциаций, антитентичность мышления, установку на разговорную интонацию.